Volume 5 - Information Technology

Proposal for Behavioral Health Services for Greater Arizona

October 2004

TABLE OF CONTENTS

Request for Confidentiality

GREABHA requests that the sections of our proposal that pertain to internet diagrams and internal network configurations remain confidential. Release of internal network and internet configurations exposes our organization's network to external attack risks. Specifically, such information (e.g., the number of firewalls, type of equipment deployed, and equipment locations) enables malicious programmers (hackers) to devise a penetration plan of attack. Although we are confident that we have adequate protections and safeguards in place, we would rather not provide publicly a roadmap to our defenses. In this matter, we appreciate the consideration of the Arizona Department of Health Services, Division of Behavioral Health Services (ADHS/DBHS).

These Sections and Diagrams have been removed from the document:

- Section A.2. Hardware and System Architecture Specifications – Arizona Service Center, Connectivity Overview diagram
- Section C.2. Architecture Design WAN diagram
- Section D.2. Wide Area Network (WAN) diagram
- Section D.3. Internet Connectivity diagram
- Section I.3. Encryption Technologies diagram

We have marked these diagrams accordingly.

a. Hardware and Software Platform

1. Overview

This proposal is being submitted by Greater Arizona Behavioral Health Authority, LLC (GREABHA), which has been established by Cenpatico Behavioral Health™ LLC (CBH), a managed behavioral health subsidiary of Centene Corporation® (Centene). GREABHA recognizes the significance of structured, expertly operated and well-maintained Management Information Systems (MIS). The MIS functions for GREABHA are managed by the MIS Department at Centene, headquartered in St. Louis, Missouri. An extensive high-speed telecommunications network links all of GREABHA's offices to the state-of-the-art data center at Centene. This data center houses the hardware, software and platform connectivity that will be used to support the Arizona Department of Health Services, Division of Behavioral Health Services (ADHS/DBHS) contract.

Centene's MIS Department enables GREABHA to effectively and efficiently manage current operations, while ensuring the ability to support requirements specific to the State of Arizona and ADHS/DBHS, including the Client Information System (CIS) File Layout and Specifications Manual, the ADHS/DBHS Program Support Procedures Manual, and the Office of Grievance and Appeals Database Manual. These systems provide GREABHA with the tools to effectively:

- Facilitate the clinical care and services for recipients
- Maintain and evaluate provider networks
- Measure the quality of care and services provided
- Manage day-to-day-operations necessary to provide the highest quality of care and data management
- Systematically adjudicate and process claim and encounter data based upon a potentially unlimited payment/block funding arrangements as well as fee for service arrangements
- Identify and resolve operational issues via system reports and extensive inquiry screens
- Comply with state and federal requirements
- Carry out other activities essential to the success of maintaining consumers' continuity of care, services and clinical outcomes

In supporting CBH behavioral health operations for other states, the MIS Department has worked with various vendors and has built a solid state government program infrastructure for managing care. The MIS staff is very knowledgeable and experienced regarding the benefits of our products, eligibility file processing, encounter processing and reporting, claims adjudication and other program related business rules.

Centene's state-of-the-art infrastructure provides the foundation to support ADHS/DBHS in its current capacities and in any expansion efforts. We have recently converted our systems to a UNIX based environment which provides us with the data warehouse structure and system redundancy that supports this capacity for growth, while also reducing system availability risk. This data structure also provides us with the ability to access any stored information needed to support the reporting requirements of ADHS/DBHS.

Centene's integrated platform leverages various systems in order to manage the delivery of these services and operational support. This information technology solution is built on the infrastructure of Centene's secure data network through use of the following systems:

AMISYS Advance (AMISYS):

AMISYS is the health care industry's premier information management system used to manage and monitor service delivery operations, encounter and claims processing and management, provide pharmaceutical data management, as well as funding administration. AMISYS is feature-rich and has well-developed functionality. AMISYS is fully integrated with clinical front-end systems used by other departments, such as Vistar's VIP used for credentialing and McKesson's CCMS used for case management.

MACESS:

- Imaging and Workflow - MACESS capabilities are leveraged for imaging any paper claims received and managing claims workflow for both electronic and paper claims.
- Service Forms – Service forms provide the ability to document, track and resolve claims related issues.

McKesson Product Suite:

The following systems provide the functionality to measure and manage the quality of care and services provided through user friendly inquiry, tracking and reporting tools:

- CareEnhance Clinical Management Software (CCMS) – CCMS supports clinical care management based on customizable criteria related to utilization management and case management while tracking this data for ease in reporting.
- Care Enhance Call Center (CECC) – CECC provides reference and management tools for our call center representatives and after-hours support staff to respond to customer needs and inquiries in accordance with identified requirements, in addition to providing reporting capabilities for monitoring purposes.

Vistar VIP

The VIP system is a highly flexible software tool used to support the credentialing process of the provider network and the many diversified relationships and contractual standards maintained.

Website (www.cenpatico.com)

GREABHA will provide a secure, easy to navigate web site to support both the provider network in managing their claims data and customers in their informational needs, in both an efficient and private manner.

Avaya:

Our phone system platform delivers call routing, advanced vectoring, messaging, and information tracking to allow for seamless and efficient call answer and service capabilities and reporting

Each of these systems and how we leverage their capabilities is explained in further detail in Section B, Operating Systems /Network Software. We maintain these systems and operate our business in a highly secure environment. Both our physical security and systems security and safeguards are detailed below and in Section I of this document. The remainder of this section details the hardware and system architecture that will be used to support the GREABHA office, its data requirements and connectivity, and details regarding the St. Louis infrastructure, which will provide the scalable and secure structural foundation for GREABHA.

2. Hardware and System Architecture Specifications – Arizona Service Center

PLEASE NOTE THAT THIS SECTION AND DIAGRAM ARE CONFIDENTIAL AND THUS WERE DELETED.

2.1. File and Print Server Specifications

The Arizona Service Center will be configured with the following hardware to support the File and Print Server, Exchange Server and Backup server:

File and Print Server specifications	HP Proliant DL380 G3 Dual Intel XEON 2.8 GHz processors 2 GB RAM System: 2- 18 GB SCSI III 15,000 RPM drives RAID 1 Data: 4- 36 GB SCSI III 15,000 RPM drives RAID 5 2- 10/100/1000 built in Network Cards
Microsoft Exchange Server specifications	HP Proliant DL380 G3 Dual Intel XEON 2.8 GHz processors 2 GB RAM System: 2- 18 GB SCSI III 15,000 RPM drives RAID 1 Data: 4- 36 GB SCSI III 15,000 RPM drives RAID 5 2- 10/100/1000 built in Network Cards
Backup Server specifications	HP Proliant DL360 G3 Single Intel XEON 2.8 GHz processor 1 GB RAM System: 2- 18 GB SCSI III 15,000 RPM drives RAID 1 2- 10/100/1000 built in Network Cards HP Ultrium 460 tape drive

2.2. Phone System

The Avaya S8300 IP PBX Media Server is an Intel based processing module that runs on a Linux operating system. The Avaya G700 Media Gateway hosts the analog, digital, IP, and trunk modules for the system. This system provides Call Center features for 450 agents. The S8300/G700 provides a complete solution for today and future telephony systems by leveraging the ability to provide analog, digital, and IP services all within one core system.

2.3. Physical Safeguards

Each remote office is secured via proximity card access on all doors. Panic switches have been installed at each reception desk. The network room inside each of these facilities is secured by either cipher locks or proximity cards.

2.4. Environmental Safeguards

The Arizona Service Center network rooms will receive independent temperature and humidity control. As in all Centene facilities, standalone portable 1 ton air conditioners or ceiling mounted 1.5 to 3 ton models will provide 24 hour control and monitoring. Standard water suppression systems will provide adequate fire protection. Power will be provided through a minimum of three dedicated circuits. Multiple APC battery backup units will be sized to provide a minimum of twenty minutes of power.

2.5. Backup Power

Backup power for remote facilities is provided by redundant APC Smart UPS systems sized to provide a minimum of 20 minutes power in the event of an outage. Redundant power supplies are installed into all routers, switches and servers. These power supplies are plugged into the redundant APC UPS and provide failover in case a power supply, APC or circuit fails.

3. Hardware and System Architecture Specifications – Corporate Office – St. Louis, MO

Centene's Data Center in St. Louis houses the main applications used to support the services and operations to support the Arizona Service Center, providers and customers. The Data Center architecture, systems and safeguards are described below.

3.1. HP Environment

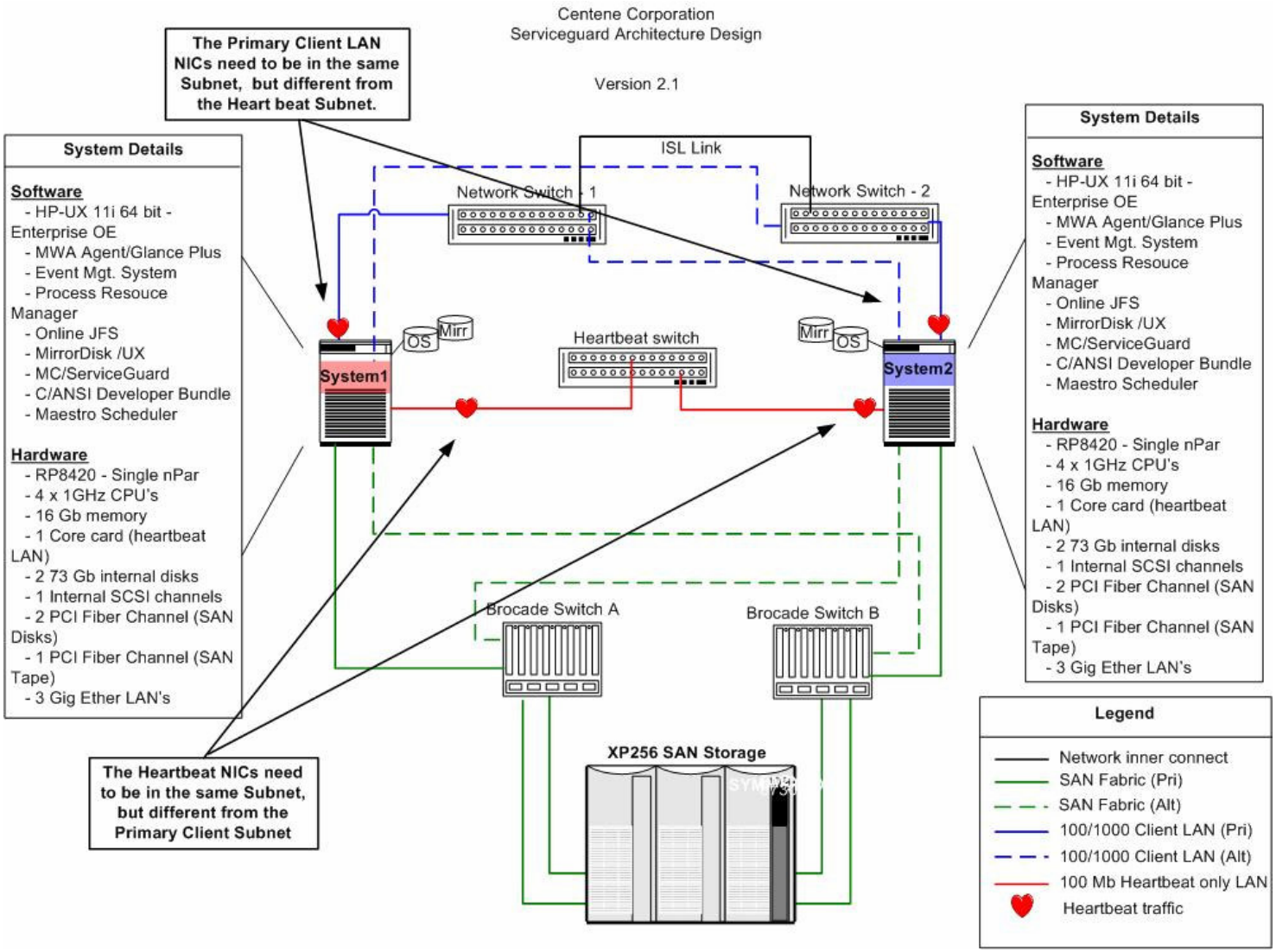
Centene's production UNIX environment is powered by two Hewlett Packard RP8420 servers running HP/UX (64-bit). Each server, fully redundant at each point of failure, stores consumer, provider and claim information in Oracle's Enterprise Server 9i database.

All data accessed through Oracle is stored on HP's XP256 SAN-attached storage. Again, fibre channels to the SAN storage are redundant in case of network loss. All data volumes are striped and mirrored for high-performance, fault tolerant data access.

Centene's high-available environment employs HP *ServiceGuard* to insure against an unplanned hardware or software outage. In the event of an outage, an alternate server is mapped to the active data volumes and ready to takeover within minutes.

3.2. Database Architecture Diagram

The diagram below illustrates the system redundancy of the HP environment on which Centene operates. Redundancies are built in the network setup such that end users will not notice any decrease in system performance should a server decrease performance. As seen below, System 1 and System 2 represent HP UNIX systems redundancy set up and availability that is supported by the Oracle data storage system. The heartbeat traffic symbol indicates where the system is monitored to ensure it is functioning properly. This heartbeat is checked every 2 seconds and if it is not detected for a defined period of time, typically less than 30 seconds, the system automatically shifts its resources to another server.


Centene Corporation
Serviceguard Architecture Design
Version 2.1
The Primary Client LAN NICs need to be in the same Subnet, but different from the Heart beat Subnet.
System Details
Software
- HP-UX 11i 64 bit - Enterprise OE
- MWA Agent/Glance Plus
- Event Mgt. System
- Process Resouce Manager
- Online JFS
- MirrorDisk /UX
- MC/ServiceGuard
- C/ANSI Developer Bundle
- Maestro Scheduler
Hardware
- RP8420 - Single nPar
- 4 x 1GHz CPU's
- 16 Gb memory
- 1 Core card (heartbeat LAN)
- 2 73 Gb internal disks
- 1 Internal SCSI channels
- 2 PCI Fiber Channel (SAN Disks)
- 1 PCI Fiber Channel (SAN Tape)
- 3 Gig Ether LAN's
ISL Link
Network Switch - 1
Network Switch - 2
Heartbeat switch
OS
Mirr
System1
System2
Brocade Switch A
Brocade Switch B
XP256 SAN Storage
The Heartbeat NICs need to be in the same Subnet, but different from the Primary Client Subnet
System Details
Software
- HP-UX 11i 64 bit - Enterprise OE
- MWA Agent/Glance Plus
- Event Mgt. System
- Process Resouce Manager
- Online JFS
- MirrorDisk /UX
- MC/ServiceGuard
- C/ANSI Developer Bundle
- Maestro Scheduler
Hardware
- RP8420 - Single nPar
- 4 x 1GHz CPU's
- 16 Gb memory
- 1 Core card (heartbeat LAN)
- 2 73 Gb internal disks
- 1 Internal SCSI channels
- 2 PCI Fiber Channel (SAN Disks)
- 1 PCI Fiber Channel (SAN Tape)
- 3 Gig Ether LAN's
Legend
Network inner connect
SAN Fabric (Pri)
SAN Fabric (Alt)
100/1000 Client LAN (Pri)
100/1000 Client LAN (Alt)
100 Mb Heartbeat only LAN
Heartbeat traffic

1

2

3.3. Phone System

The Avaya S8300 Media Server is an Intel based processing module that runs on a Linux operating system. The Avaya G700 Media Gateway hosts the analog, digital, IP, and trunk modules for the system. This system provides Call Center features for 450 agents. The S8300/G700 provides a complete solution for today and future telephony systems by leveraging the ability to provide analog, digital, and IP services all within one core system.

3.4. Physical Safeguards

The Centene core communications and telecommunications systems are housed in a secured data center at the Centene Corporate office located in Clayton, Missouri. The building is first secured at the elevators with proximity card access required to access all secured floors. Proximity card access also protects all entry doors per floor. The data center itself is secured by an additional layer of proximity card access which is given only to specific IT and IS Operational staff members. All visitors and vendors must be accompanied by an IT or IS Operations staff member while in the data center. The proximity cards are individually assigned to employees by our Security Department and must be worn at all times while in the office. All access to doors, elevators and the data center is monitored, recorded and audited by our Security Department. Centene provides two on-site security guards during business hours. Panic buttons have been installed at each reception location in the building.

3.5. Environmental Safeguards

The Primary Data Center is temperature and humidity levels are controlled through two Liebert high capacity precision air conditioning systems. Both systems are tied into Centene's security system and send an audible and remote alarm when temperature or humidity falls outside of the predefined ranges or water is detected via the drip sensor. Multiple wireless temperature sensors are also placed throughout the data center and provide a constant remote display at the desks of the IT Director, IS Operations Director and WAN Engineers.

A FM200 fire suppression system is schedule to be installed in the Data Center in early 2005.

3.6. Backup Power

Power for the data center is conditioned through redundant Liebert units which provide over two hours of backup power. A backup diesel generator with 5,000 gallon fuel capacity for the data center is expected to be installed 4th quarter 2004.

b. Operating System/Network Software

1. Overview

Centene provides the technical expertise and support as needed to fulfill the systems requirements needed for GREABHA to appropriately manage its contractual obligations. This includes maintaining the operating system and network software, performing system updates as warranted, as well as developing custom programs to meet requirements. The breadth and depth skills of the MIS department, as illustrated in Section G, IT personnel training, is also proven through previous and current management of systems used to support significant Medicaid business. The MIS team continually seeks ways to improve processes and enhance system performance to produce the most effective means of accomplishing these obligations.

This section details our operating systems, software applications and ability to customize a solution for ADHS/DBHS and system update processes.

2. Operating Systems

Centene's database design provides the flexibility and extensibility needed to access and develop informational needs to meet ADHS/DBHS requirements. While Centene Corporation owns the source code to certain of the software applications, there may be times when custom code is developed to accomplish business objectives. AMISYS, in particular, while having robust capabilities inherent in the system, also allows us to customize programs that are accessed through a user exit program to run external processes that satisfy these objectives. Skilled programmers within the MIS department program custom code in various languages that support our ability to meet or exceed ADHS/DBHS requirements.

2.1. Software Platform

The platform and programming languages used by the MIS department to manage the various operating systems are outlined in the table below:

Application	Database Structure	Vendor	Source*	Programming Language(s)
AMISYS Advance	Oracle	AMISYS Synertech	Yes	COBOL, Powerhouse, Suprtool
MACESS	N/A (proprietary)	SunGard	No	N/A (proprietary)
CCMS	SQL	McKesson	No	EC Map, SQL, VB6
CECC	SQL	McKesson	No	EC Map, SQL, VB6
VIP	SQL	Vistar	No	PowerBuilder
Website	SQL	N/A	Yes	HTML, ASP, J2EE, CSS, Photoshop, Flash, Java Script, VB Script

* Indicates ownership of the application's source code

2.2. Desktop Operating System

Desktop systems currently run Windows 2000 Professional, Service Pack 4. The standard configuration package includes Microsoft Office 2000 Professional, Minisoft and Network Associates ePolicy Orchestrator Enterprise agent running McAfee Virus Scan 7.0. The operating system and all files are secured through NTFS permissions.

3. Software Applications and Ability to Customize

The Software Applications to be used by GREABHA to support this contract were identified in the Overview in Section A. These systems integrate tightly through the use of a back-end data storage facilities that retain various and large quantities of data and information such as consumer, provider, encounter, status, and case management activity and outcomes. Furthermore, the front-end case management database accepts select data transferred from these back-end data storage systems to provide the representative with a comprehensive set of information to effectively and properly manage the consumer's and provider's needs.

Detailed usage of each of these tools is provided below to further outline the flexibility and extensibility of the Centene infrastructure that will support ADHS/DBHS. Each of these tools is highly customizable to satisfy ADHS/DBHS' business requirements. Our ability to customize each of these systems is discussed in each item.

3.1. AMISYS Advance

Following are the main AMISYS subsystems and modules that will be used to meet the requirements of this contract:

- Enrollment / Membership and Eligibility Processing – Electronic and data entry
- Benefits Management
- Provider / Contract Processing
- Pricing
- Third Party Reimbursement Processing/Liability Recovery
- Encounter / Claims Processing and Adjudication
- Batch Processing
- Financial Management / Fund Accounting/Premium Billing & Accounts Receivable
- Reporting
- Interface Management
- Security

AMISYS's extensive functionality will be leveraged to ensure the data quality and management of funding streams according to the Arizona's block funding model

Enrollment / Membership and Eligibility Processing

Centene supports the enrollment interfaces required by ADHS/DBHS, as well as HIPAA 834 file processing requirements. GREABHA will administer the enrollment interfaces by applying written procedures and automated scripting to transfer data via BBS or FTP supported processes.

The MIS department has created mapping/translation programs for loading membership, which link eligibility status to all AMISYS subsystems. The mapping programs take the eligibility files, which are in the HIPAA ANSI Standard Format, validate each data item and map each data item to the AMISYS standard membership batch input file format. Centene then uses the batch membership interface subsystem to further validate, cross-check and load the membership data (i.e., recipient and provider ID numbers, recipient name and DOB and demographics, Contract, Benefit and PMP info, etc.) into the main AMISYS tables, where the data is accessible from all subsystems.

To increase operational efficiencies, the batch load process identifies possible duplicate recipients, as well as other errors and warnings, and produces an error report to Eligibility Specialists. The Eligibility Specialist follows up on any instances where eligibility is questionable. Once all the batch errors are corrected, the eligibility records are loaded into AMISYS. This automated process effectively adds, deletes, and modifies the consumer records in the GREABHA database. Eligibility files can be processed daily, weekly, bi-weekly or monthly. Current enrollment and disenrollment data is stored according to the consumers' start and stop

dates. Date sensitive consumer history information is also stored and accessible. Thus, GREABHA personnel will be able to access the length of time that each consumer has been enrolled as well as the reason for a consumer's disenrollment.

Enrollment information is quickly and effectively transmitted electronically, in accordance with Centene policies and procedures. Our subcontractors are required to verify GREABHA eligibility information. As required by ADHS/DBHS, AMISYS's enrollment subsystem will maintain GREABHA's historical data (files) indefinitely.

Benefits Management

GREABHA's transactions with providers will be paid in compliance with Federal and State law and regulations. The MIS Benefits subsystem will be configured to reflect services deemed covered and non-covered by ADHS/DBHS. If at any time a code has been deemed by ADHS/DBHS to be moved to covered or non-covered status under ADHS/DBHS' programs, AMISYS can be updated to reflect this change and allow for proper claim processing resolution.

Provider /Contract Processing

AMISYS stores provider data in a number of provider dataset records that are all linked by the Provider ID number. A variety of provider contract scenarios can be configured to reflect group verses individual provider agreements. AMISYS provides the ability to manage multiple office locations and practices to which a provider may belong. These records are then linked to the provider. The Provider subsystem also accommodates providers who have multiple financial arrangements. Unique provider records are created in accordance with each provider's name, Tax ID number and Medicaid ID (AHCCCS ID). GREABHA will submit all provider changes through the contract workflow administered by GREABHA's Provider Contracting Department.

The MIS system allows for payment restrictions on providers paid on a fee for service basis, who are suspended from GREABHA's network for fraud or abuse. Such providers are placed on review in AMISYS, which holds all payments for the provider's claims during the time period he/she is under investigation by ADHS/DBHS or its authorized agent(s). If a provider has been suspended, the claims system can be set to deny or pend claims submitted by that provider.

Providers are given written notice regarding each claim/encounter that has been processed, including a description of the acceptance or rejection reason on an Explanation of Payment (EOP). Alternatively, a letter may be sent at the time of the acceptance or rejection if the claim cannot be entered in the claim system, or if the rejection needs more clarification, or if additional information is needed.

Pricing

The MIS system will maintain ADHA/DBHS's provider fee schedules via AMISYS's Provider and Pricing Subsystems and will allow for fee schedule updates based on data provided by ADHS/DBHS. Historical fee schedule data is also maintained in AMISYS for reference. The pricing subsystem can be configured to price according to fee schedules, per diem rates, capitation, block funding scenarios and many other complex pricing arrangements.

The pricing process determines the correct affiliation for the servicing provider and the associated pricing arrangements, with respect to the date of service on the submitted claim.

Third Party Reimbursement Processing / Liability Recovery

The Coordination of Benefits (COB) department tracks and maintains a history of other coverage by constantly updating other insurance information that is housed in the Other Insurance

Coverage (OIC) listed in Member Alternative Coverage (MAC) screen in AMISYS. This information is gathered either from the Explanation of Benefits (EOB) or through an investigative phone call to the potential other insurance company when there is reason to believe OIC exists. The COB department is responsible for ensuring that effective and term dates of the OIC as well as all personal information is accurate (by way of the phone call). It is also an ongoing function to make sure that all family members' OIC information is up to date in our system. When other insurance information is present in AMISYS the system recognizes the date of service for that particular encounter and compares it to our MAC screen to determine if other insurance is involved for that date. Having the system identify encounters in this manner allows the COB Team the opportunity to look at potential COB savings even when an EOB is not attached.

Encounter Submissions / Fee for Service Claims Processing and Adjudication

To support GREABHA, the MIS Department utilizes a combination of the MACESS workflow system, the AMISYS Batch Claims Processing Subsystem and the AMISYS claims processing subsystem to process encounter submissions and fee for service claims. The system will be specifically designed to comply with ADHS/DBHS, its appointed agents and federal requirements to process encounters and claims for Arizona Behavioral Health programs. Centene has the capability to capture and utilize data from both internal and subcontracted sources, as well as interface with other systems as necessary, such as the ADHS/DBHS or its fiscal agents to meet administration and reporting requirements. Our system allows for the collection and reporting of all encounter data, financial information and administrative reports required by ADHS/DBHS.

All services to GREABHA consumers, even those provided by block funded or capitated providers, will result in the submission of an encounter/claim form. GREABHA is acutely aware that:

- Accurate encounter data needs to be submitted to ADHS/DBHS in a timely manner.
- The timely and accurate processing of claims for payment is critical to ensuring that providers continue to make services available and accessible to consumers.

GREABHA will monitor and manage the processing of this data to ensure that the standards set forth by ADHS/DBHS are met in accordance with the requirements and timelines of Client Information System (CIS) File Layout and Specifications Manual, the ADHS/DBHS Program Support Procedures Manual and the Financial Reporting Guide for Regional Behavioral Health Authorities.

Batch Processing

Batch encounters/claims can be entered online or by electronic transmission. The Batch Claim Processor edits encounters/claims and services in the batch database for valid data. It also:

- Validates fields and adjudicates claims
- Invokes edits from the six main subsystems
- Moves the encounters/claims into the main HEALTH database
- Assigns the appropriate status or resolution (i.e., paid, denied, denied for additional information claims, rejected, denied due to a duplicate claims, or internally pended)

Encounters/claims that are internally pended are processed through online claims processing subsystem screens. All other accepted and finalized records generate an Explanation of Payment (EOP) is created for each provider.

Financial Management / Fund Accounting/ Premium Billing and Accounts Receivable

AMISYS capabilities provide for fund tracking and reporting in accordance with the block funding and funding stream management requirements indicated in the ADHS/DBHS requirements documents. The system is highly configurable in conjunction with the Pricing sub-system to

support block funding arrangements. The system allows for the designation of which funding entities hold the payment for an encounter or claim based on various criteria. This allows for accurate reporting and tracking of payments for fund accounting. Claim payments and reported encounters are drawn against funding entities as defined by ADHS/DBHS. AMISYS data feeds the Finance Department's systems for billing and accounts receivable processing as outlined in the Finance Department Support section later in this document.

Reporting

AMISYS provides for a very robust reporting environment. Several options are provided within the standard AMISYS application to allow for user invoked/requested reports. In addition to the standard report options, AMISYS's database stores all data in a manor that expedites the capabilities for custom report generation. Centene's Applications Development staff has access and in-depth experience with the AMISYS databases, and can efficiently create new, or modify existing custom reports in order to meet or exceed ADHS/DBHS reporting requirements. Reporting needs are met primarily through one of three options. The first two options are standard in AMISYS and are standard reports produced through either the Standard Report Menu or the Custom Reporting Report Menu. Depending upon the deliverable, additional reporting requirements can be met using other data extraction tools or CareEnhance Clinical Management Software (CCMS), which is described later in this section.

GREABHA will follow all ADHS/DBHS standards for data format, data element, transmission, and schedule standards, including the monthly submission of encounter data. We will ensure that all required data elements are included in each submission, including encounter data adjustments. GREABHA will use all codes specified by ADHS/DBHS, including, but not limited to, procedural and diagnostic codes. GREABHA is willing and able to provide ADHS/DBHS with all requested data both in standardized reports and special requests, as needed by ADHS/DBHS. We will consistently respond to standard and special requests for reports and information..

Interface Management

The Interface Subsystem is comprised of a combination of customized processes built by Centene programmers and AMISYS's standard data interface subsystem. Because AMISYS is a fully integrated managed system, it supports both incoming and outgoing data from any internal or external party. AMISYS contains a central database comprised of multiple, unique tables. The tables contain detailed information regarding claims, consumers, providers, procedure codes and other pertinent information. For example, the health database contains the service table, where claims are stored, and the provider table stores demographic information regarding the provider. Although there are many tables in AMISYS, there are subsystems that allow access to these tables. These subsystems access the same tables that prevent data from being duplicated. We have developed an interface solution that allows rapid processing of consumer, claim and encounter data from any business partner or subcontractor in any format and can standardize it before it reaches the AMISYS tables. Centene currently supports daily, weekly, monthly, bi-monthly, quarterly, annual and ad hoc transactions of all types to and from our business partners. GREABHA will make use of these reports in fulfilling our management needs and ADHS/DBHS requirements.

Security

AMISYS Security is detailed in our response to Section I, System Security and Audit Trail.

3.2. MACESS

MACESS provides the functionality to make our processes efficient with its process management, documentation and tracking functions.

Imaging and Workflow

MACESS is the imaging and workflow system used to aid in the efficient management of customer service functions. The MACESS system provides:

- HCFA and UB form scanning
- OCR functionality
- Data entry and electronic queuing and tracking of claims
- On-line communication between the call centers and claims with Service Forms
- Electronic filing of all claims received by GREABHA

AMISYS also provides on-line and batch processing of all received encounters/claims. In an on-line environment, the subsystem automatically verifies eligibility, calculates co-payment or deductible amounts (as appropriate) and validates codes at the time of entry. In the batch mode, encounters/claims are entered into the system via electronic media either from an EDI clearinghouse or from the MACESS system, subjected to edits, and pended or processed for payment based on user-defined criteria.

Service Forms

MACESS provides an efficient and effective on-line communication mechanism between the call centers and the service department with its Service Forms feature. Service Forms are used to correspond with others within GREABHA and Centene, as well as to document issues and any actions needing to be taken for the resolution of those issues. Service forms become permanent records in consumer and provider folders, once entered into the system.

3.3. McKesson Product Suite

Centene uses the McKesson Product Suite as its front-end case management for use by the call center and after hours customer service and provider support. These systems are leveraged to perform many functions, such as workflow management, and call tracking and reporting, which are identified below.

GREABHA will monitor the development and composition of the Treatment Teams using CCMS functionality to ensure that clinical liaisons and family and natural supports are in place for consumers

CCMS

- Centene uses CareEnhance Clinical Management Software (CCMS) to automate workflows and customize clinical decision support criteria related to utilization management and case management. CCMS allows us to:
- Integrate utilization, case and disease management efforts
- Proactively identify, stratify and monitor high-risk populations
- Consistently determine appropriate levels of care and efficiently document the impact of our programs
- Helps leverage data regarding consumers of services
- Pinpoint where care is needed
- Implement customized intervention strategies
- Provides a mechanism for the production of letters that programmatically pre-populate with appropriate data to meet ADHS/DBHS requirements.

We have the ability to incorporate ADHS/DBHS clinical necessity criteria for Level 1 services, which can easily be tracked within CCMS. CCMS combines utilization and case management into a seamless process and improves communications among care managers for better outcomes.

CECC

CareEnhance Call Center (CECC) software is used by the call center and accessed by the after-hours staff to provide reference material and tools for providing appropriate support to providers

and consumers. This includes scripting, call and follow-up call tracking, consumer contact information, provider profile data, assessment surveys, educational materials, triage guidance, specialist referral information, and class registration management. In addition, the software includes the following capabilities:

CECC can be configured to support patient outreach and outcomes monitoring

- Tracking Patients' Privacy Preferences – A patient's indication that he/she does not wish to receive further calls from the program can be captured.
- Policies and Procedures to Ensure Patient Privacy - While all employees receive training in the protection of patient-identifiable information as part of their orientation, these preferences are available on CECC as additional reinforcement. These policies define which confidential patient information can or cannot be disclosed and under what circumstances.
- Data Access – Call center personnel have real-time connectivity to the case management database on Centene's dedicated server in the St. Louis corporate office. Data is imported into CECC from the AMISYS database and updated nightly.
- Messaging Center – The communications capabilities within CECC include the ability for the case manager to track and send information to patients in a variety of methods, including mail, fax or e-mail.
- Reporting – Routine reports, such as profile data, will be produced and mailed to providers.

3.4. Vistar - Credentialing Software

Privileging of family support partners will be configured in the VIP system in compliance with ADHS/DBHS guidelines

Both flexible and responsive, the Vistar VIP system is designed to accommodate the many diversified relationships and contractual scenarios dictated by today's managed care industry. Managing different client requirements is possible while still sharing primary physician data in accordance with credentialing standards. The VIP system will be used to support ADHS/DBHS with its functionality to track credentialing and privileging information, including that for non-licensed providers. It will also be used to track training activities completed by these providers.

System functionality and services include unlimited notes, unlimited images and unlimited data lines. Credentialing is never forced to drop history or data because there are not enough fields to accommodate the information. The system has unlimited user defined fields and up to nine additional user defined screens for entity level use. The System Options function allows system administrators to hide fields, set system defaults and pre-set automatic processes on a user level, permitting GREABHA to define and re-define data elements and system functionality.

Centene has configured the VIP system to provide users with the following additional features:

- A simple Query by Example and Ad-Hoc Query Search Feature, which allows users to search in any field(s) and to use a simple Summary List for quick and easy reports
- Capabilities to search on any field and any screen (table) in the system. Multiple fields and screens can be included in one search to provide an unrestricted perspective related to file maintenance
- Sophisticated ticklers, expiration reporting and mass processes that ensure verification is completed in accordance with national standards
- Imaging functionality throughout the system functions.
- Sophisticated entity and access filters built in to security and practitioner profiles that allow records to be categorized in numerous ways. A practitioner can have primary data verified

once and can view details for multiple contracts on the same record. NPDB reports can be generated for each EIN number in compliance with NCQA standards.

- Multi-level security: Security can be assigned or removed by user, group or organization
- Users can be set up with various access ranging from full update rights to view only.
- Both user actions and administrator actions are stored in the Audit Trail Functions

3.5. Website

GREABHA will provide an easy to navigate web site with Arizona specific information and functionality for use by providers with enhancements scheduled to increase provider functionality and serve consumer informational needs. The web site does not require tools or techniques that require significant memory, disk resources or special intervention on the customer side to install plug-ins or additional software. In addition, a specific browser will not be required in order to access the web site. The CBH website address is www.cenpatico.com. Upon contract award, GREABHA will establish a similar website.

The GREABHA website will provide information such as:

Topic	Content
About GREABHA	Detailed information about the including strategic partners, mission, management, news releases, history and contact information
Quality reports	Contains PDF files illustrating our strong quality review results on various topics
Programs / Services	Description of the programs and services we currently offer
Provider Tools	Each state in which we do business has provider information to help providers doing business with GREABHA: • Provider Directory and Forms • Provider Announcements

Enhancements focused on consumer informational needs will include the following:

- Information on how to access behavioral health services including crisis contact information
- Consumer Handbook and Educational Information
- Customer Service Contact Information and Hours of Operation
- Advocacy Organizations
- Health and Wellness Information
- HIPAA Privacy Notice

The site will comply with the Americans with Disabilities Act.

In addition, the GREABHA website will be expanded to include a secure provider environment that will allow a provider to:

- Verify Eligibility
- Inquire into the status of encounters/claims and Level 1authorization request.

3.6. Phone System - Software

We utilize various Avaya software tools to support our call centers: We utilize Avaya's Communication Manager Version 2.1 as our advanced software platform that delivers world-class call routing and feature rich applications. All of our call centers are managed through automatic call distribution (ACD) and advanced vectoring.

Avaya's Call Management System Supervisor Version 11 is our Call Center reporting system that tracks information processed through ACD. An Intel/Linux based Sun Sparc Server is the hardware platform. Seamless collaboration is provided via network connection to ACD features in the switch. CMS uses a graphical user interface application to collect and report call traffic data, and format management reports. Data is presented in both real-time and historical formats.

Avaya's Intuity LX Version 1.1 is the multi-media messaging platform that allows users to respond to messages via voice, fax, text and file attachments. An Intel/Linux based server is the hardware platform.

Finally, ISDN-PRI circuits provide the trunking capabilities from the local exchange carriers and national long distance vendors. These circuits allow additional information to be carried to the call center agent. 800 numbers are provided for inbound call routing. In addition to the ISDN-PRI, networked DS1 tie trunks are able to be utilized in company wide dial plan along with providing high volume and emergency routing. This provides a reliable backup method in call routing.

3.7. Finance Department Support

Centene's MIS Department supports the Finance Department through the use of state-of-the-art systems and software listed below:

- ***MultiView:*** Centene utilizes MultiView software to record and report financial data. All financial transactions are auditable per GAAP guidelines and historical data can be obtained from MultiView through the use of queries and reports. These queries and reports are used to help generate budgets and projections.
- ***Freedom:*** Centene uses Freedom software to report quarterly and annual statutory filings to agencies such as NAIC and ADHS/DBHS. Freedom has the flexibility to inter-face with our Sungard Enterprise Portfolio System (EPS) software for schedule D reporting on the statutory filings. Enterprise Portfolio System is an investment management system that provides comprehensive accounting and reporting information for GREABHA.
- ***AMISYS:*** Through the utilization of AMISYS, GREABHA has the ability to administer standard reports, as well as engineer data various ways to create supplemental reports for compliance with state reporting regulations..

In addition to recording and reporting financial information, Centene's third party auditor, PricewaterhouseCoopers, LLP ensures that all Centene subsidiaries, of which GREABHA is one, are in compliance with Generally Accepted Accounting Principals (GAAP) and statutory accounting principals.

4. System Updates

Centene manages software upgrades and service pack updates through a controlled Change Management Process. While the parallel systems for programming and testing are outlined in the Change Request process covered in Section F, History of Downtime, this section outlines the business processes followed in the Change Management Process. Some Service Pack updates occur automatically, as is further outlined in the Service Pack Updates subsection below.

4.1. Change Management Process

A formal change request process tracks changes or new work requested and monitors results from these requests to ensure quality review and documentation of the changes being made. This

process provides an organized method to handle system customization requests and modification requests efficiently and effectively. Centene's MIS Department actively monitors this process through a tracking software tool, which also allows stakeholders to review progress on the request. Key process steps include:

- Initiate the Change Request (CR) –User request changes by providing necessary supporting documentation to illustrate the issue.
- Senior Management Approval - Appropriate Centene senior management, staff and MIS representatives must review to validate necessity, appropriateness and impact of the change.
- Estimate of Work - Designated representatives estimate and prioritize changes requests according to impact and value added based on documentation provided in the initial request.
- Business Analysis - Once assigned, the CR is owned by a Project Manager to analyze the business and systems impacts of the change.
- Approach Design - The Project Manager then coordinates the configuration and programming design and changes with the appropriate resources.
- Testing - The MIS department performs unit, regression and as appropriate end-to-end testing of the proposed changes before submitting for user acceptance testing.
- User Acceptance Testing - Various interested parties review and approve test results and may perform additional testing.
- Production Control - As changes pass testing, the MIS department produces a schedule of the job for the Operations department. The operations process is outlined in Section F.
- Production Release - IS Operations executes the new program according to scheduling software
- Post Production Management - Completion of jobs is monitored and production errors or issues are managed by the programming staff that is available at all times

4.2. Service Pack Updates

Microsoft Software Update Server is configured to automatically download and install approved service pack updates and patches to all desktops in the organization on a nightly basis. In addition, the MIS staff continuously reviews, plans and upgrades other system software. This ensures that users remain current with new releases and make the most of available functionality:

- All software is kept under vendor maintenance contracts, which provide support for diagnostic assistance, upgrades, fixes, new releases, documentation and notification of developments.
- Software and system upgrades are coordinated to ensure that there is no disruption to operations or users. Our MIS Executive Management Team reviews proposed changes and establishes priorities including schedules for development and installation.
- Proposed upgrades impacting the Arizona program will be submitted to DHS for prior review and approval in accordance with DHS guidelines as outlined in Special Terms and Conditions, Paragraph I of the RFP.
- All changes are fully tested on our development environment before being released into production. Users also participate in testing the upgrades, thus enabling accurate testing of the system functionality and the procedures that are integrated into the system.
- Failure alerts are reported to Computer Associates' Unicenter. Critical events trigger email and/or text paging notifications to WAN engineers.

c. System Compatibility

1. Overview

Centene's capacity to maintain strong connections between our MIS offices, ADHS/DBHS and GREABHA providers is demonstrated in the strength of the technical foundation of our infrastructure, as illustrated in previous sections of this document and further outlined below. While our goal is to encourage as much electronic interaction as possible, we will support the submission of paper claims as well:

- We have the ability to interface with external parties using various software packages and mediums.
- We have the ability to support both incoming and outgoing data by the use of our Electronic Bulletin Board (BBS) system called Wildcat Interactive Net server.
- Our business partners can pick up and drop off files at any hour of the day, seven days a week.
- We do not require the business partner to have any special communication software package to use the BBS system.
- If our business partner is unable to use our BBS system, we have the staff support to use the business partner's BBS system instead.
- If our business partner does not have a BBS system, we can send and receive secure files through the Internet, e-mail, tape, diskette, or CD.

This section identifies provider system support including the foundation of our architecture design needed to begin, inbound and outbound data flow, paper claims submission process, reporting, provider remittance and status reporting and technical assistance for providers.

2. Architecture Design

1 **PLEASE NOTE THAT THIS SECTION AND DIAGRAM ARE CONFIDENTIAL AND THUS WERE DELETED.**

3. Inbound and Outbound Data Flow

In addition to the technical infrastructure needed to support the providers, Section E, Ability to Provide a Secure Data Electronic Data Interface, describes our ability to interact electronically through bulletin board systems and the diagrams in the Data Flow section of this document illustrate the data inflows, core processes and data outflows that comprise the Centene support structure for data exchange between Centene and the providers. These data inflows and data outflows make the process as efficient and effective as possible using current technology.

4. Paper Claims Submission Processes

While we strive to process information as efficiently and effectively as possible through electronic means, we understand that sometimes paper processing is necessary.

As previously mentioned, we use a combination of the MACESS workflow system, the AMISYS Batch Claims Processing Subsystem and the AMISYS claims processing subsystem to process paper claims. The system will be specifically designed to comply with ADHS/DBHS requirements.

Centene's Claims Processing Department has been processing claims for over 15 years and achieves high standards for accurate and timely claims payment. Daily audits are performed to ensure that the claims staff meets internal accuracy goals of 100 percent production and 95 percent quality.

Currently our turnaround time for claims payment is as follows:

- 98% of all claims are paid or denied within 14 days, and 99.9% within 30 days.
- The average length of time for a claim to be paid from date of receipt is six days.

Per standard policy, Centene processes all provider claims in a timely, accurate and efficient manner and issues payment for all covered services within 30 days of receipt for all clean claims. Centene's claims transaction system has prepayment reporting capabilities that allow review of 100 percent of all claims specific to a provider at the request of ADHS/DBHS. All manual and automated system procedures and processes are documented in standard Policy and Procedure documents.

The paper claims process flow is described and diagramed in Section K, System Data Flow. Once the claims are processed to a pend, pay or deny status, MACESS is updated to reflect this within the queue process. Resolved claims are set to a payable status; however, the CSC staff is managed through queues that outline the pended claims process flow as discussed later in this document. The MACESS IMAX interface allows for effective management of pend queues electronically instead of paper tracking processes. A processor simply opens their desktop and works through their claims issue work queue.

5. Reporting

As mentioned previously and illustrated in the stability and core system structure, GREABHA leverages the Centene integrated systems infrastructure through the use of a data storage facilities that retain various and large quantities of data and information regarding the consumer, provider, utilization, status, etc. These data storage facilities provide GREABHA with a comprehensive set of information to effectively and properly manage the provider's reporting needs. Through the use of this data structure, GREABHA has the ability to perform both patient and provider profiling to:

- Monitor a patient's treatment utilization patterns to detect over or under utilization in identified key areas such as inpatient or pharmacy
- Identify gaps between care recommended and care received
- Combine data such as key clinical indicators in addressing over or under utilization in a single integrated "patient profile" for use by providers and case managers
- Illustrate to providers in a "physician profile" their individual success in following evidence-based practice guidelines for care
- Report in a way to allow GREABHA the ability to appropriately pay providers based on quality-of-care outcomes achieved
- Compare provider performance results to averages across all ADHS/DBHS providers for the same measures
- Focus on clinical practice pattern indicators to evaluate the quality of care provided in assuring providers follow nationally accepted practice guidelines

Reporting capabilities will include the ability to compare encounter data against care management plan data to ensure providers are meeting access to care standards, such as the seven day initial appointment standard

6. Provider Remittance and Status Reporting

In addition to the processing of paper claims for payment, providers may submit encounter data for inclusion in ADHS/DBHS reporting as part of this contract. In order to successfully work together with ADHS/DBHS and systems used by providers, Centene practices clear and open communications so that information is accurately submitted and reported. Two elements of this communication and reporting are encounter processing and status reporting.

6.1. Encounter Processing

Centene recognizes the importance of encounter processing and reporting and has dedicated personnel and hardware to ensure efficient, timely and integrated performance. As noted in other sections of this document in detail, the AMISYS system can collect, transmit and receive all of the

data required related to consumer eligibility, providers, encounters, capitation and remittance. Centene's systems can maintain Consumer demographic and historical eligibility information including associated behavioral health benefit package level and historical services provided with associated cost.

Other sections describe Centene's claims submission processes, including methods to ensure timely and accurate claims adjudication and payment. Using data on eligibility, benefits, providers and authorizations, a system with multiple checks and balances has been established in pursuit of timely and accurate claims adjudication. Centene's encounter reporting process makes use of this data through Centene developed programs to build encounter files for submission. This process uses ADHS/DBHS standards to guide programming to include the needed data elements, needed file formatting and transmission mode.

The development of encounter files results in a series of reports to insure data integrity, timeliness and completeness. These processes are outlined in the System Data Flow section of this document under Section K. As discussed previously, all services to consumers result in the submission of a claim form. Centene is acutely aware that timely and accurate processing of these claims is critical to ensuring that providers continue to make services available and accessible to consumers, and that accurate encounter data is submitted to ADHS/DBHS. Centene identifies, monitors and manages the processing of claims to ensure that the encounter processing standards are met.

6.2. Standard Explanation of Payment

The Explanation of Payment (EOP) is a printout sent to providers that shows the amount paid to a provider for services rendered to a consumer. The report also lists the procedures performed and amount paid by the organization for the services. GREABHA has the ability to produce this report at any time. This EOP is generated through the Claims Payable Subsystem of AMISYS.

Our standard policy provides for GREABHA to process all provider claims in a timely, accurate and efficient manner and issues payment for all covered services within thirty days of receipt for all clean claims. Our claims transaction system has prepayment reporting capabilities that allow review of 100% of all claims specific to a provider upon authorized request.

7. Technical Assistance for Providers

GREABHA Provider Training and Assistance teams will be established and staffed with highly skilled technical and business professionals, who will be dedicated to meeting and exceeding the requirements of this contract. These teams will be available to help providers handle inquiries and requests for application support. In addition, a full staff of analysts and programmers are available to handle enhancements through the Change Management Process outlined previously.

d. Network Configuration and Architecture

1. Overview

Designed to support both our current business environment and expansion opportunities, our system configuration provides both the stability and strength to meet the needs in supporting ADHS/DBHS. This section includes a description and diagram of both our Wide Area Network (WAN) and our Internet Connectivity.

2. Wide Area Network (WAN)

PLEASE NOTE THAT THIS SECTION AND ASSOCIATED DIAGRAMS ARE CONFIDENTIAL AND THUS WERE DELETED.

3. Internet Connectivity

PLEASE NOTE THAT THIS SECTION AND ASSOCIATED DIAGRAMS ARE CONFIDENTIAL AND THUS WERE DELETED.

e. Ability to Provide a Secure Electronic Data Interface

1. Overview

Centene has the ability to securely interface with external parties, including providers and ADHS/DBHS, using various software packages and mediums. Centene strives to increase the electronic exchange of data in order to create the most efficient method of doing business with partners and clients. An EDI team is dedicated to the continuous support of ADHS/DBHS, providers and clearinghouses in support of the electronic processes. In addition, a proactive approach is taken by contacting providers submitting paper claims to inquire about EDI capabilities.

In addition, Centene is structured to respond to any ad hoc electronic data submissions, processing or review requests from DHS within the required 30 day notice timeframe.

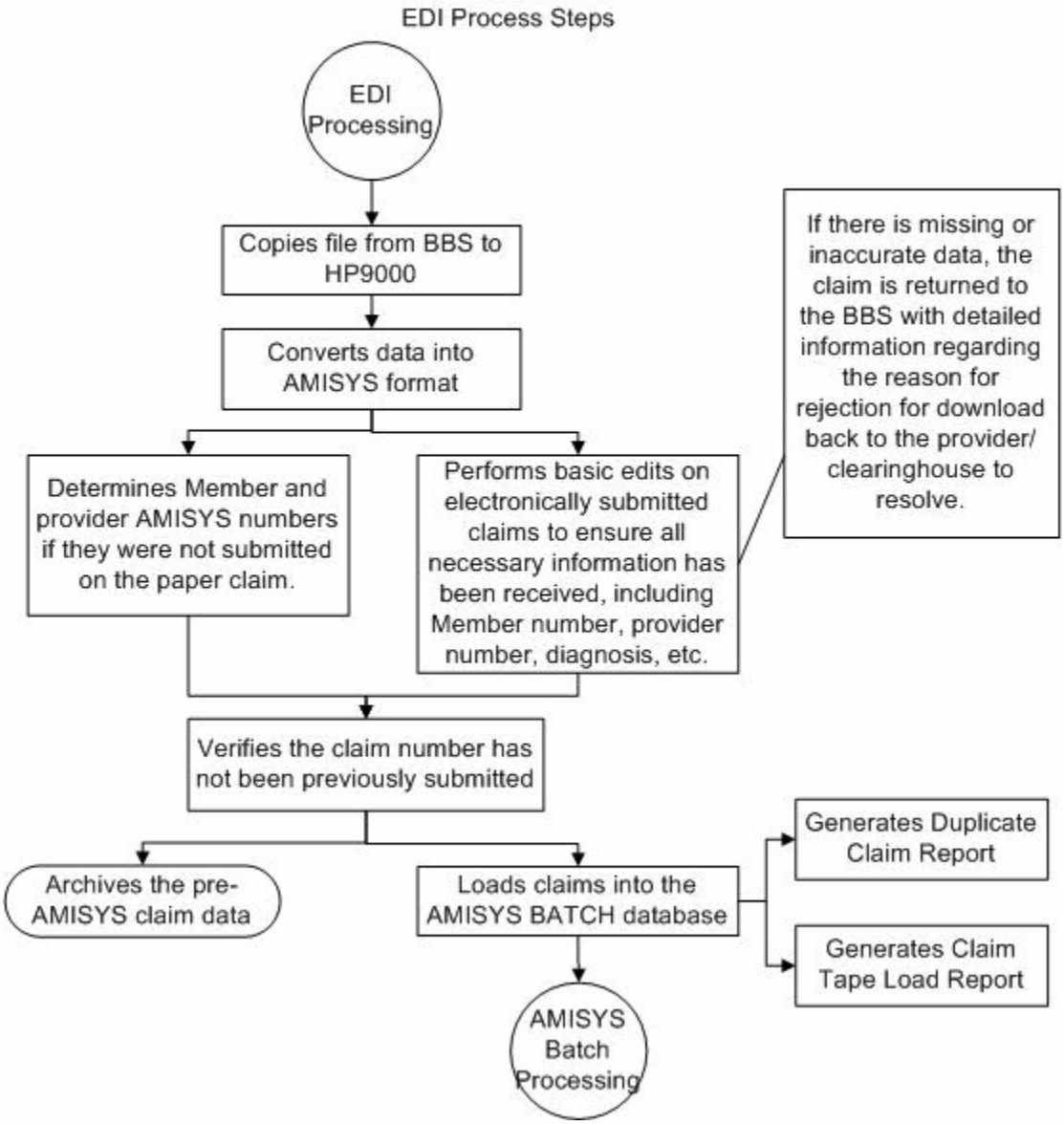
2. Software Mediums

Centene supports both incoming and outgoing data through the use of our Electronic Bulletin Board (BBS) system, called Wildcat Interactive Net server. Wildcat enables Centene's business partners to pick up and drop off files at any hour of the day, seven days a week. Business partners do not need to have any special communication software packages in order to use the BBS system. If a business partner is unable to use the Centene BBS system, Centene can use the business partner's BBS system instead. If the business partner does not have a BBS system, Centene can send and receive secure files through the Internet, e-mail, tape, diskette, or CD.

2.1. File Flow - In

When the claim or claim data has been uploaded from the BBS, it is ready to go into EDI processing. All claims go through the EDI process for the validation of critical pieces of information on the claim. Before claims are moved into the BATCH database of AMISYS, electronically submitted claims are checked for pertinent information. Each claim passes through data validation processes before it reaches the AMISYS system. The EDI process copies the claim files from the BBS to the HP9000 and prepares the claim files for entry into the AMISYS Batch Claims Processing system.

This process is illustrated in the diagram below and described further in the detailed process steps outlined below the diagram:



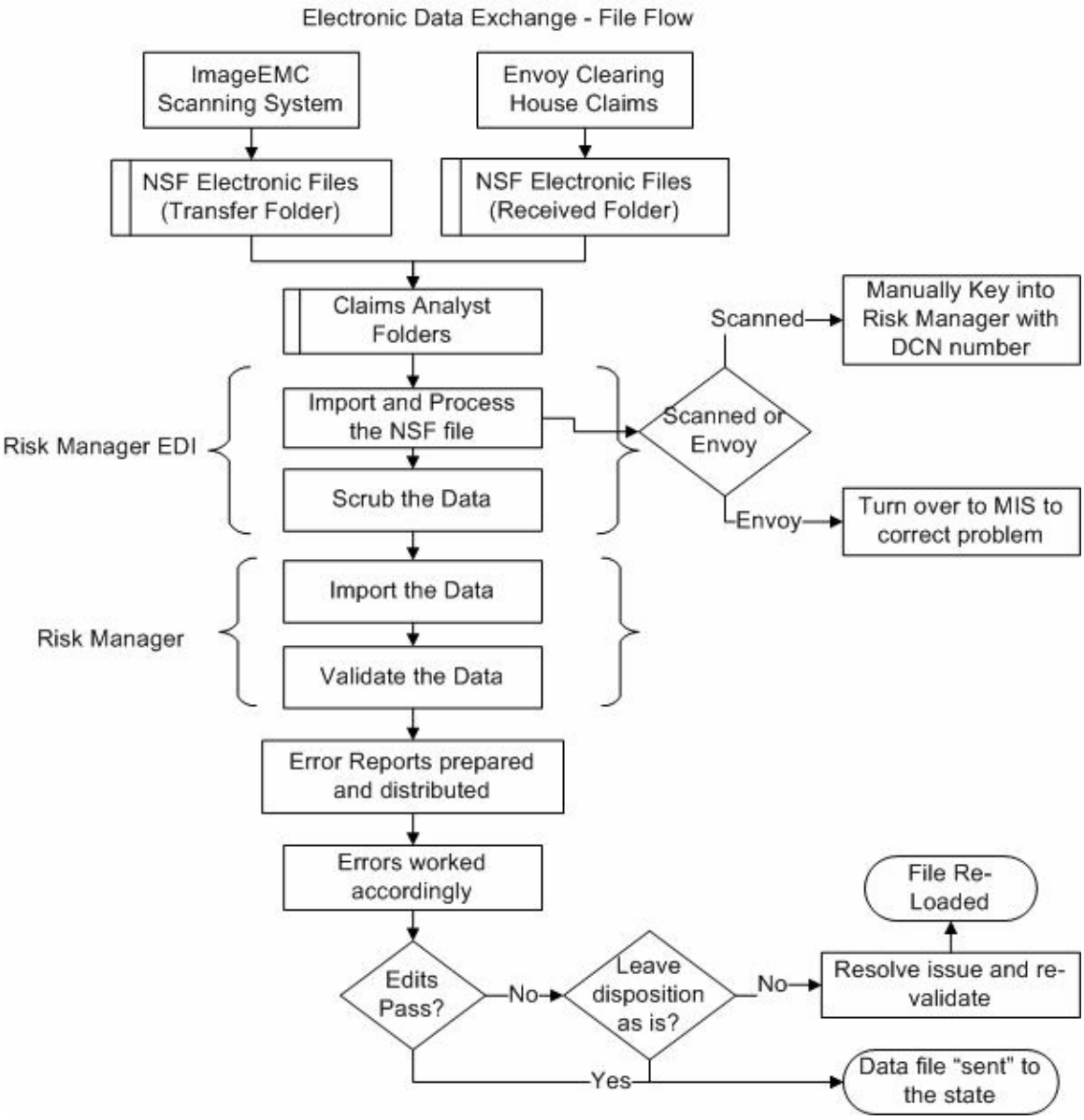
Process steps include:

- The data is converted into an AMISYS-ready format.
- The EDI Program performs basic edits to verify all pertinent information is present and accurate. If a claim is submitted with incomplete, inaccurate, or missing data, it is rejected and returned to the BBS in the form of an error file within 24 hours. The provider/clearinghouse downloads error files to resolve these errors. Claims rejected based on these edits can be resubmitted electronically.
- Clean files are loaded into the AMISYS BATCH database and a detailed report of data loaded into batch is generated.
- The EDI program then archives the pre-AMISYS claim data as part of the quality control process.
- The clean file is generated and loaded into the AMISYS BATCH database for processing.

Processing occurs twice a day, Monday through Friday. Files received prior to 4:00pm MST are processed the same day.

2.2. File Flow – Out

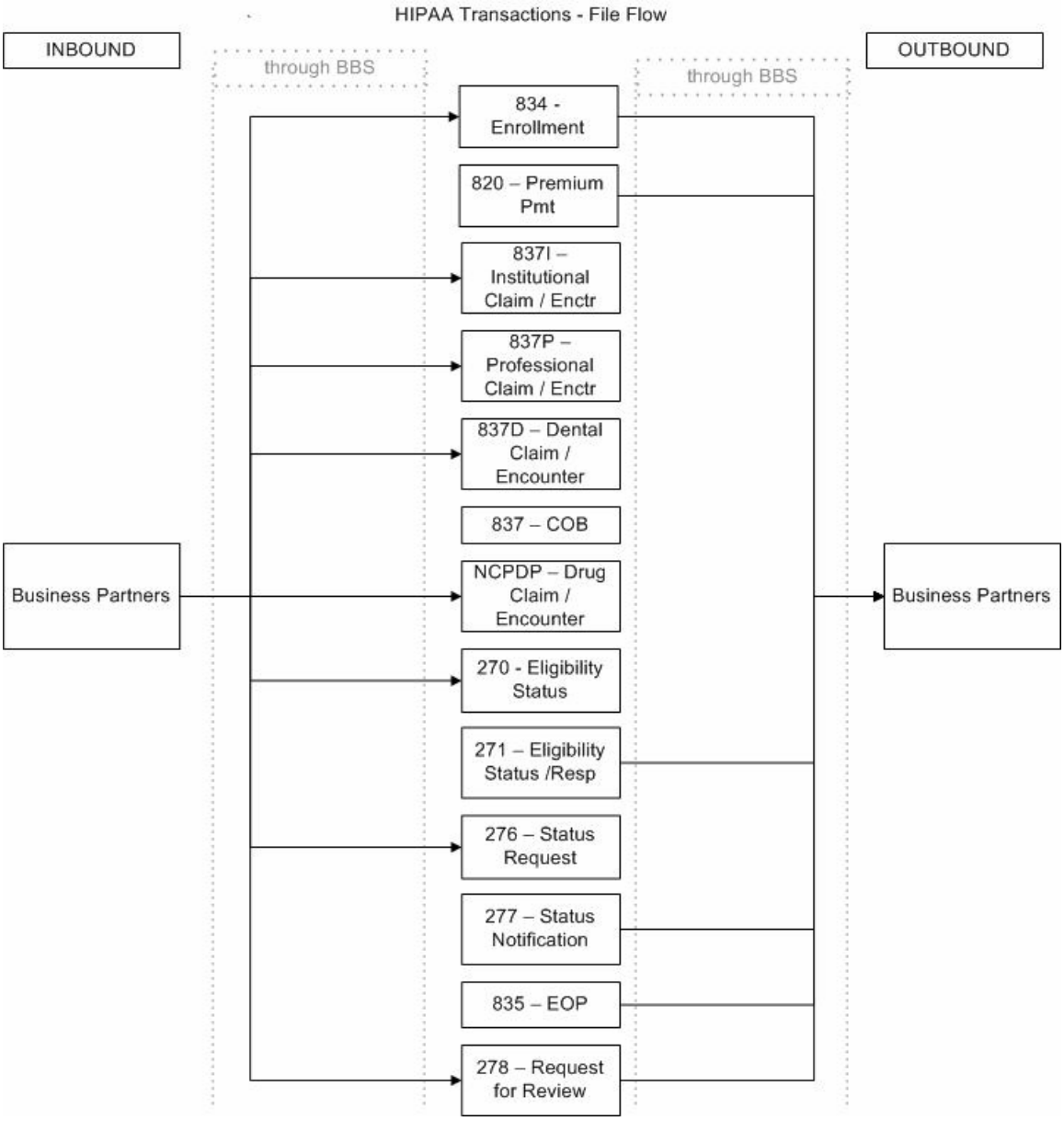
The following diagram illustrates the flow of files and the scrubbing process for a file to be posted or sent to ADHS/DBHS:



HIPAA Compliant Transactions

Centene complies with applicable certificate of coverage and data specification reporting requirements promulgated pursuant to HIPAA. In order to comply with these requirements, Centene has invested in translation software, EC Map, in order to map, translate and compliance check inbound and outbound HIPAA transactions. Centene has a proven record or successfully implementing several of the HIPAA transactions.

The following diagram visually illustrates the HIPAA transactions Centene is able to support:



3. Other Transactions

Centene is willing to build the reasonably appropriate mapping and capabilities to support other electronic transactions for ADHS/DBHS. This includes the ability to accept electronic data from DHS regarding:

- The status of AHCCCS eligibility applications that have been sent by behavioral health providers into Arizona Dept. of Economic Security/Family Assistance Administration and AHCCCS Central Screening Unit
- Fraud & Abuse, IMD, Seclusion and restraint, Incidents, accidents, deaths, Enrollment, Disenrollment & other data submissions

4. HIPAA Certification

Centene has received certifications from EDIFECS that the 837I and 837P files are HIPAA compliant:

f. History of Downtime

1. Overview

The MIS department strives to ensure minimal disruption in systems availability to support the functional areas of the entire organization. The stability of our system and its availability is proven by the detail provided below covering scheduled downtime, unscheduled downtime, system availability, and parallel systems.

2. Scheduled Downtime

AMISYS Production

Over the past 6 months, all Centene accounts that operate the AMISYS software were upgraded to AMISYS version 11.01 from version 10.00. Additional memory was installed on the production system in order to improve performance.

Over the past six months the local power supply to our data center has been upgraded to accommodate the implementation of a backup generator. The system has been extremely stable, and despite these major initiatives, the product has been available for use 98.44% of the time.

CCMS

Over the past six months Centene has conducted two major upgrades to the CCMS infrastructure. In April 2004 the database was migrated from SQL 7 to SQL 2000. In July 2004 the system was moved to a new hardware platform with dual processors 2.8 GHz Xeon processors and 2 GB of RAM. Additionally, the local power supply to our Data center has been upgraded to accommodate the implementation of a backup generator. The system has been extremely stable, and despite these major initiatives, the product has been available for use 98% of the time.

E-Mail

Over the past six months the local power supply to our data center has been upgraded to accommodate the implementation of a backup generator. The system has been extremely stable and despite these major initiatives the product has been available for use 99% of the time.

WAN

Over the past six months the local power supply to our data center has been upgraded to accommodate the implementation of a backup generator. The system has been extremely stable, and despite these major initiatives, the product has been available for use 99% of the time.

3. Unscheduled Downtime

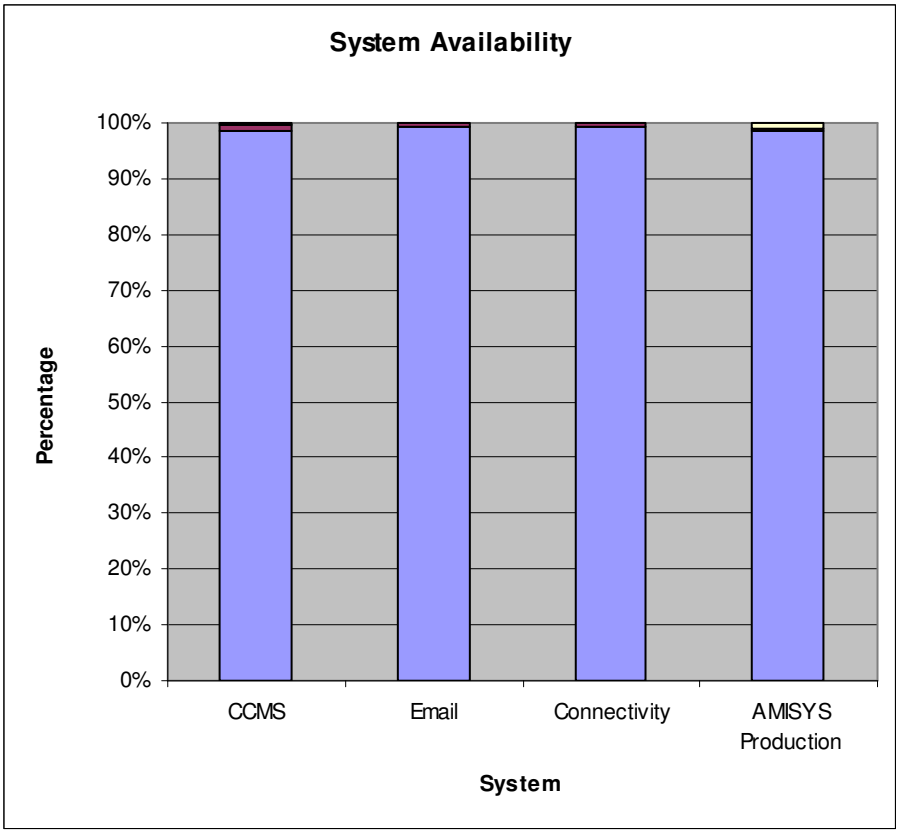
Over the past 6 months, the AMISYS production server on which GREABHA business is running lost 36 hours due to hardware problems, three hours due to bad XP256 array card, and three hours for a power outage. The local power supply to the computer room has been supplemented by the installation of a backup generator.

4. System Availability

The following chart illustrates the availability of our production systems for the period March 2004 through August 2004:

SYSTEM AVAILABILITY

	CCMS	Email	Connectivity	AMISYS Production
Available	98.42%	99.36%	99.36%	98.44%
Scheduled	1.21%	0.55%	0.55%	0.61%
Unscheduled	0.37%	0.09%	0.09%	0.96%



5. Parallel Systems

5.1. Process

The MIS department uses parallel systems to maintain the integrity of the production system at all times. It also utilizes testing resources from various impacted areas to manage the development, testing and production release of source code changes in a structured manner.

The production control process ensures that only approved changes get released into the production systems on a scheduled basis:

- The system source code is first “checked out” by the programmer who is making the changes.
- When a programmer has “checked out” a source code program, it cannot be checked out by another programmer at the same time.
- The programmer makes the requested changes to the program, moves the compiled program to the development environment to perform their own unit testing and requests testing to be performed by business users accordingly. This environment is a replica of the production environment, which enables the business to perform change testing as well as regression testing to the extent necessary.
- Once the changes have been approved, the Programmer completes a Production Control Form to request the tested and appropriately labeled source code to be moved into the Production Environment by the Operations staff.
- The Operations staff is then responsible for moving the source code into the production environment according to the deployment schedule and in accordance with the instructions provided in the Production Control Form.

5.2. Hardware

The following chart lists the hardware configuration currently used to support our AMISYS production and development/test servers:

Production Server Specifications	HP9000 RP8420 • HP-UX 11i 64 bit OS • Amisys App/DB Servers (Prod) • Cell Boards = 1 (PA8800) • Actvive CPU’s = 4 x 1GHz • Memory = 16 Gb • Disk = 2 x 73 Gb Int.
Development/Test Specifications	HP9000 RP4440 • Amisys App/DB Server • HP-UX 11i 64 bit O.S. • Cell Boards = 1 (PA8800) • Actvive CPU’s = 2 x 1Ghz • Memory = 8 Gb • Disks = 2 x 73 Gb Int.

g. IT Personnel Training

1. Overview

Our goal is to attract, develop, challenge and retain the best and brightest talent available. Quality of our people is one of our keys to success. To this end, Centene's Training Department, continually updates and upgrades opportunities for all employees, focused on identifying the core competencies that together make up a profile for success for individuals and the entire organization. We recognize the importance of training in creating an ideal work environment, raising the confidence and abilities of employees and improving the ability of the company to support the consumers we serve. In accordance with this philosophy, staff is offered several levels of initial and ongoing training.

This MIS department specifically recognizes the significance in developing its employees both with respect to the Medicaid products we support as well as in the current technologies needed to succeed. This section describes both job-specific training and the general training that is offered to all employees, including the MIS personnel. In addition, we have provided a list of the specific courses taken and certifications achieved by current personnel to illustrate the broad skill set of this group.

2. General Employee Training

The Training & Development Department is committed to four major goals and objectives:

- Develop a competency-based Human Resources Management (HRM) system.
- Develop and implement a standardized new-hire training checklist for each position.
- Expand the use of web and computer-based training to reach a broader audience at less cost and higher quality.
- Continuously evaluate training and development needs, and expand opportunities.

2.1. Computer Based Training

General new employee training is conducted locally by key Centene staff, and includes an overview of Centene operations. Employees participate in extensive Computer Based Training (CBT) that includes the following CBT courses:

Name of Course	Course Description
Demo Course	Familiarizes users with web based training
Centene Overview	General description of Centene Corporation, including company history and senior leadership
Diversity & Anti Harassment	Mandatory training explaining diversity and anti-harassment guidelines
Compliance	Mandatory training describing Centene's corporate compliance philosophy and programs
HIPAA Training	Mandatory consumer privacy training
Preventing Workplace Violence	Mandatory training to prevent violence in the workplace
Cultural Competency	Mandatory overview of cultural differences, similarities, styles, and an appreciation of these cultures, with emphasis on the influence of culture on health care decision making.

Name of Course	Course Description
Member Services Overview	Overview of the services extended to our consumers and providers through this department – telephone inquiry, education, etc.
Care Coordination Overview	Overview of the services available to our consumers and providers – Disease Management, Utilization Management, referrals, pharmacy, etc.
Policies & Procedures	Overview of MHS policies and procedures
Finance Overview	Brief overview of the Finance Department's roles and responsibilities
Employee Benefits Overview	Explanation of employee benefits, valid as of June 1, 2004, and updated annually or as benefits are enhanced

2.2. Classroom/Hands-On Training

Centene offers on site classroom training in the subsidiary offices as well as in the corporate offices in newly designed training rooms with state of the art technology. Courses vary from technical to business management. Business courses include Centene Leadership Institute (CLI) and Centene Academy for Leadership Excellence (CALE), which are designed for executives, managers, and supervisors, as well as Train-the-Trainer courses for employees performing on-the-job or standup instruction to other employees.

2.3. Other Training Opportunities

Other Training Opportunities include:

- Regularly offered "Lunch and Learn" seminars, whose materials are available on-line
- Materials such as videos and presentations from the classroom training courses are available to all employees interested in self-study.
- The SALSA program, a standalone skills assessment that Centene utilizes to test employees on their PC skills
- CBT learning, provided by a partner organization, Mindleaders.com. Includes courses in areas such as computer skills, technical skills, compliance, job knowledge, time management and conflict resolution
- Training on Centene Policies & Procedures
- Educational assistance through a 100% tuition reimbursement program

3. MIS Specific Employee Training

Training programs for the MIS personnel are tailored according to individual roles and responsibilities to ensure current technology, systems and process education. These programs are provided both upon initial employment as well as on an ongoing basis to ensure retention.

3.1. Hands-On

Following of some examples of the type of hands-on training made available to MIS personnel:

AMISYS Advance Configuration training	• Various courses and certifications are offered in the AMISYS sub-systems we use: • Membership and Benefits Management • Capitation Payable • Indemnity Configuration • Claims Processing • Pricing Management

AMISYS Advance Technical Orientation	• This course provides a foundation for learning the software layers and utilities that make up the AMISYS Advance system, through lecture and hands-on activities to cover such topics as: • Architecture Structure and Working in the UNIX Environment • UNIX File System and Directory Structure • Directory structure and UNIX File Commands/Utilities • File redirection, and piping – file characteristics, permissions and access rights • Oracle and SQL

3.2. Shadowing

Mentoring is also a key component of the training program. Upon hire, a new IS/IT employee is assigned to a mentor who is available for questions and to provide guidance on the way Centene programs and configures its systems to meet the needs of our clients. In addition, the new employee is scheduled with various cross-functional experts to learn about their specific areas. Such training typically includes the following:

Area	Description
General Training	• Overview of the Training Plan • Centene 101 (topics identified in general training section above) • Voice Mail system
AMISYS: One-on-One Training	• AMYSIS Inquiry • System Maneuvering and System Searching • 6 Steps to Adjudication • Issue Resolution vs. Service Status • Membership/Benefits/Provider/Pricing/Claims Overview • Utilization Management Overview
Core Processes: One-on-One Training	• Eligibility/Remittance • Claim Flow – paper (MACESS) and electronic (EDI) • Claims Payable • Web Sites • Encounter Processes • CECC/CCMS/VIP/CRMS • HIPAA Compliance
HP Environment: One-on-One Training	• HP Machines & Passwords • MPE Commands • Vista Folder Functions • Reflections and QEDIT Overview
IS Programming: One-on-One Training	• JCL Overview • Maestro Intrinsics • Cobol/Supertool/QTP Overview • IS Operations Overview • Adager • MHSDB database • Data Dictionaries: PHD and MHSDB • AMISYS Databases • Source/Compile Matrix • Version Control • Programming Standards • Reflection Scripts • Documentation Procedures • Production Control Form (PCF)
IS Administrative	• CR Process, Time Tracking and MISC Tracking Numbers • On Call Procedures – Daily & Evening

Area	Description
Office Visits	• Farmington and MDC Office for Functional Overview

1 4. IS/IT Qualifications

2 Continuing education and certification is highly encouraged for our MIS department personnel.
3 Courses taken and certifications received by our employees are listed below.

4 4.1. Certifications

5 Following is a list of certifications held by one or more of our employees:

Area	Description
Novell Certifications	• Certified Network Engineer Version 3, 4 and 5
AMISYS	• Programmer Migration Training • Benefits • Billing and AR • Capitation Payable Subsystem • Claims Payable, Pricing and Code Review • Promatch • Technical Orientation • 1099 Processing • Correspondence Generator • Cypress
Microsoft Certifications	• Microsoft Certified Professional • Microsoft Certified Professional plus Internet • Microsoft Certified System Engineer 3.51, 4.0,+ Internet, +2000 • Microsoft Certified Trainer
Cisco Certifications	• Cisco Certified Network Associate and Professional • Certified Information Security Systems Professional
CompTIA Certifications	• A+ • Network +
Telecommunications Certifications	• ACACN - Avaya Certified Associate Communication Networks
Other Certifications	• Certified Technical Trainer and Dell Hardware Certification

6 4.2. Education

7 In addition to the courses taken as a new employee as listed in this question's response,
8 following is a list of additional courses taken by our one or more of our employees:

Area	Description
Cisco Courses	• Interconnecting Cisco Devices • Building Scaleable Cisco Networks • Cisco Multilayer Switching and Internet Troubleshooting • Cisco Secure PIX Firewall Advanced and Cisco Works
Telecommunications	• ARS • Vector • Advanced Vector • Administration • Cisco Cvoice and Voicemax
Programming	• 837I and 837P • Accelerated SQL • Alchemy Database

Area	Description
	• Assembler I & II • C and C++ • COBOL I,II,III, IV • DBII • ECGateway • FoxPro • HTML and WEB Programming • Java I & II • Certified Data Base Administrator-IBM • SQL Fundamentals Using Oracle • SQL programming using SQ Server • SQL -RAD Environment Certified • Oracle Programming using PL/SQL I & II • UNIX 9000 UNIX SQL training • Visimage/Vital Soft Ware • Visual Basic
Microsoft Courses	• Install, Configure and Administer Microsoft Windows 2000 Professional • Install, Configure and Administer Microsoft Windows 2000 Server • Implement MS Windows 2000 Professional and Server • Implement and Administer a Microsoft Windows 2000 Network Infrastructure • Implement and Administer a Microsoft Windows 2000 Directory Services Infrastructure • Manage a Microsoft Windows 2000 Network Environment • Design a Microsoft Windows 2000 Directory Services Infrastructure • Design Security for a Microsoft Windows 2000 Network • Design a Microsoft Windows 2000 Network Infrastructure • Install, Configure and Administer MS Exchange 2000 Server • Design and Deploy a Messaging Infrastructure with MS Exchange 2000 Server • Install, Configure and Administer Microsoft SQL Server 2000 Enterprise Edition • Design and Implement Databases with Microsoft SQL Server 2000 Enterprise Edition • MS Office Product Suite: Word, Excel, PowerPoint, Visio, Access, Project • Microsoft Project Enterprise Administrator • Microsoft Project Management Solution • MS Windows 9x support
Software	• CCMS and CICS • Pricing/McKesson and MACESS • Team track and Team track Administrator
Business Courses	• (ICA) International Claim Assoc. • (PAHM)Prof. Academy of Healthcare MGMT • Business Communications and Centene Supervisor Institute • Management Skills for New Managers, Supervisors and Tech. Supervisors • Project Management -Understanding the PM Role • Myers-Briggs Training and 7 Habits of Effective People • Essentials of Credibility • HIAA Parts A,B & C Group Life & Health • HSS-Healthcare Software Synergies • Provider Contracting & Guidelines Training • Sexual Harassment • Leadership Training • Writing Class AAIM • Centene Behavioral Interviewing • Signature Service Training
Other	• OS2 Warp Admin

h. System Data Archive and Retrieval

1. Overview

GREABHA has the necessary hardware and software to meet, and in many cases exceed, the ADHS/DBHS Management Information Systems requirements for managing, collecting, transmitting and storing all of the data elements required under the contract. In the event of either a complete systems failure or catastrophic event preventing normal business operations needing these systems and data, the MIS department is ready and equipped to support the recovery in an expedient fashion. This section identifies the processes in place to support this recovery and includes the entire plan approach as well as the MIS specific responsibilities as part of the entire Business Continuity Plan. First we discuss the data archive and retrieval process for accessing data in the event of systems failure, then we further detail the recovery plan and processes followed to ensure business continuity in the event of a catastrophic event.

2. Data Archive and Retrieval

Backups are performed on a nightly basis using Backup/3000 by Orbit, which provides fast and reliable online backup on any size MPE/iX system. The tapes are archived at a secure off-site, storage location. If production data restoration becomes necessary, the archival log is checked for the proper set of tapes. A tape-return request to the secure off-site location is initiated. Once the tapes are onsite, the appropriate data restoration procedures are selected and applied.

Special features include:

- Fast store and restore operations
- Zero down time back-ups, which enables all data files, including Image, AllBase and Oracle, to be backed-up without taking users off-line, and which enables the MIS Department to backup only that data in the file that has changed since the previous back up
- Multiple tape drives, with parallel backup and restoration functions, support DLT and 8mm tape drives, tape manager and librarian for tracking tape usage and file placements on backup and disk to disk backups

Full system backups are performed on a nightly basis. The tapes are then sent to an off-site secured storage location.

Centene provides a dedicated stand-alone backup server for each plan office. HP Netservers running Computer Associates Brightstor Enterprise Backup utilize internal or external Ultrium 460 tape drives for LAN based backups.

Full backups are performed on all LAN based servers on a nightly basis. A “Grandfather, Father, Son” tape rotation is used with a five week cycle. Daily tapes are held for 35 days, monthly tapes are held for 18 months and yearly tapes are held indefinitely. Tapes are rotated offsite daily to a secure, climate-controlled, fireproof facility. For security reasons, recovery of the tapes is limited to selected GREABHA personnel. In the event of an emergency, the backup tapes can be recovered from the secure backup facility in one hour.

Centene’s Operations staff has developed all manual and automated procedures for all processes that the MIS Department undertakes. All procedures are kept online in a DATAGUIDE that is kept up-to-date as changes are made. This has proven to be an efficient system for ensuring all processes. For example, Eligibility, Remittance, State Deliverables are completed by due dates and in a timely manner. The Operations staff also has automated scripts, which

automatically pick up files from the BBS system and or Arizona FTP sites and places them on the HP9000 or network drives for processing.

3. Business Continuity Plan

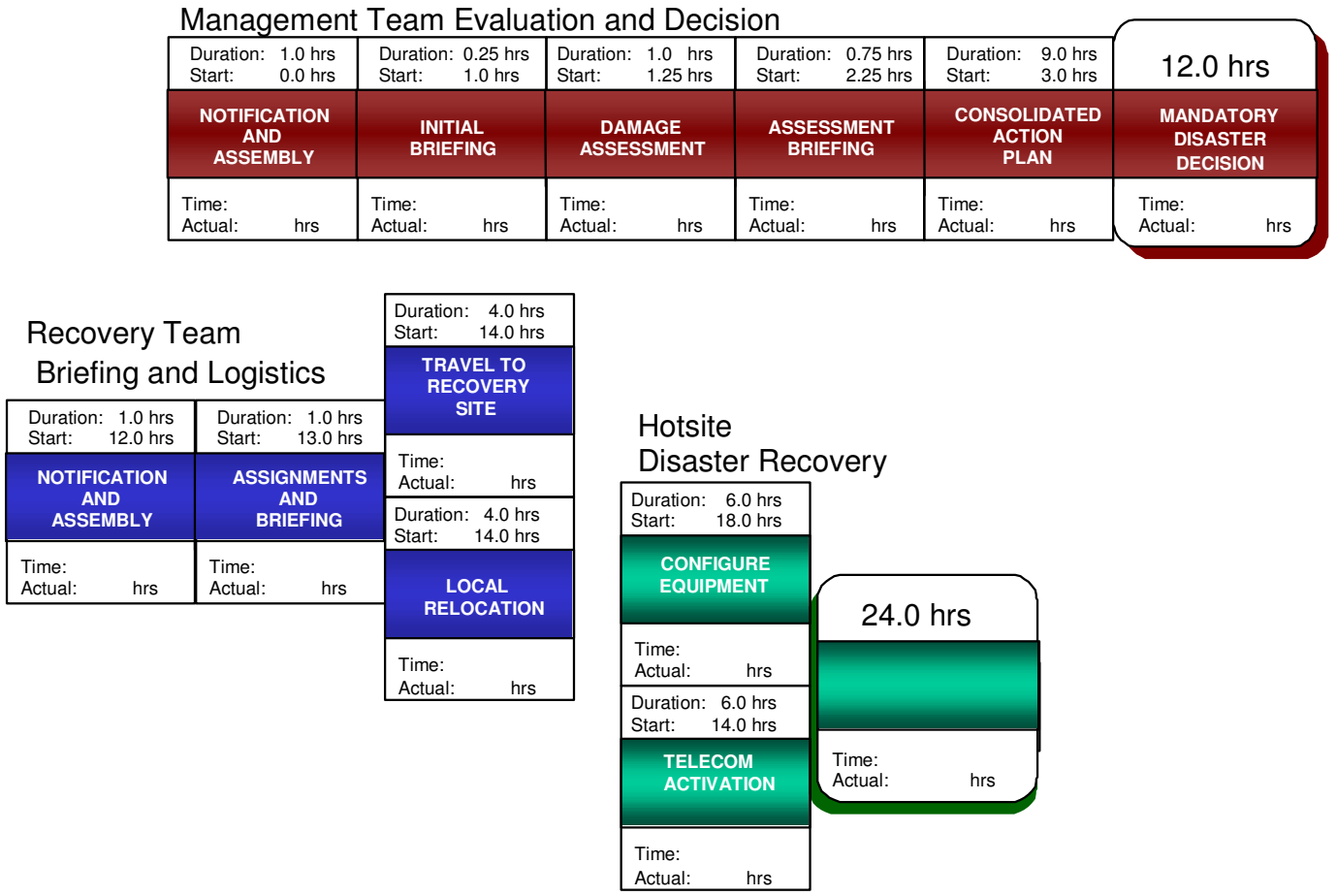
3.1. Approach and Timeline

Centene subcontracts with SunGuard Planning Solutions, Inc. for Disaster Recovery Plan (DRP). The DRP uses a recovery team format, and is organized as a combination disaster time checklist, reference document, and training aid. The various milestones, tasks, and procedures are based on the incident circumstances and approved Consolidated Action Plan (CAP). The CAP summarizes the specific strategies and selected actions to address the particular incident and is developed at the time of the incident.

The Recovery Plan was developed to meet these specific objectives:

- Provide an organized and consolidated approach to managing response and recovery activities following any unplanned incident or systems interruption, thereby avoiding confusion and reducing exposure to error
- Provide a prompt and appropriate response to any unplanned incident, thereby reducing the impacts resulting from short-term business interruptions
- Recover the business functions, represented as the responsibilities of the recovery teams listed in the Recovery Organization Table, below, in a timely manner and reducing the time during which the Corporate office is unable to conduct business
- Recover Information Systems and data network environment in a timely manner, increasing the ability to recover from a damaging loss to the facility

Following is the recovery timeline used to monitor actual recovery activities against projected timelines:


Management Team Evaluation and Decision
Duration: 1.0 hrs
Start: 0.0 hrs
NOTIFICATION AND ASSEMBLY
Time:
Actual: hrs
Duration: 0.25 hrs
Start: 1.0 hrs
INITIAL BRIEFING
Time:
Actual: hrs
Duration: 1.0 hrs
Start: 1.25 hrs
DAMAGE ASSESSMENT
Time:
Actual: hrs
Duration: 0.75 hrs
Start: 2.25 hrs
ASSESSMENT BRIEFING
Time:
Actual: hrs
Duration: 9.0 hrs
Start: 3.0 hrs
CONSOLIDATED ACTION PLAN
Time:
Actual: hrs
12.0 hrs
MANDATORY DISASTER DECISION
Time:
Actual: hrs
Recovery Team
Briefing and Logistics
Duration: 1.0 hrs
Start: 12.0 hrs
NOTIFICATION AND ASSEMBLY
Time:
Actual: hrs
Duration: 1.0 hrs
Start: 13.0 hrs
ASSIGNMENTS AND BRIEFING
Time:
Actual: hrs
Duration: 4.0 hrs
Start: 14.0 hrs
TRAVEL TO RECOVERY SITE
Time:
Actual: hrs
Duration: 4.0 hrs
Start: 14.0 hrs
LOCAL RELOCATION
Time:
Actual: hrs
Hotsite
Disaster Recovery
Duration: 6.0 hrs
Start: 18.0 hrs
CONFIGURE EQUIPMENT
Time:
Actual: hrs
Duration: 6.0 hrs
Start: 14.0 hrs
TELECOM ACTIVATION
Time:
Actual: hrs
24.0 hrs
Time:
Actual: hrs

3.2. Team

As mentioned, the disaster recovery plan was developed using a recovery team format. The GREABHA disaster recovery teams will acquire support from other Business Units by contacting the Centene Corporate Office Incident Management Team during an incident.

Following are the disaster recovery teams that are in place for CBH's Austin Service Center. Following contract award, a similar team will be established to handle disaster recovery for the Arizona Service Center.

CBH	TEAM LEADER	ALTERNATE
Executive Management	Beth Mandell	Greg Shulman
Incident Commander	Edward Vasquez-TX	Greg Shulman
Recovery Coordinator	Cindy Peterson-TX UM Staff Edward Vasquez-TX CS Staff	Greg Shulman-TX
Utilization Management Customer Service	Cindy Peterson-TX Edward Vasquez-TX	Ginger Arizola-TX Laura Knowlton-TX
Administration	Edward Vasquez-TX	Greg Shulman-TX

The Business Units with identified roles:

LOCAL SUPPORT FUNCTIONS	PRIMARY CONTACT	ALTERNATE CONTACT
Facilities Management	Jim Rey	Dave Roser
Finance	Brian Butts	Anna Lawniczak
HR/Personnel	Mary Sanchez	Marcia Bequette
Legal/Regulatory	Jennifer Spears Dawn Crumel	Centene Corp. Office
Office Services / Mail Room Support	Les Moss	Heather Biron-TX
Travel/Transportation Services	Carlson Wagonlit Travel	24 hours 800 number
Data & Voice Communications	Keith Bernier	John Colvin

CORPORATE SUPPORT FUNCTIONS	PRIMARY CONTACT	ALTERNATE

		CONTACT
Public Relations/ Corporate Communications	Suzanne Hall	Cary Hobbs
Insurance Support	Melissa Arbet	Cindy Jansky

3.3. Process

The Management Team provides overall coordination of response and recovery support activities.

Plan Activation Procedures document the initial evaluation, decision, and team activation activities performed by the Management Team. The team provides specialized coordination and communication of all incident response. Specifically, these procedures include:

- Activating the appropriate incident support personnel
- Assisting in developing the Consolidated Action Plan (CAP)
- Mobilizing any subordinate recovery teams

Notification of a potentially disruptive incident may come from a variety of sources, depending on the nature of the incident and time of day. Initial response to the notification may be dictated by company emergency response procedures and standard operating practices.

These recovery processes are based on a worst-case disaster, such as total destruction or loss of access to Centene's offices requiring recovery at alternate work locations. The Management Team acts as a central clearinghouse to:

- Coordinate available resource allocations among the associated Recovery Teams. Requests for resources and logistical support are funneled through this team to the appropriate support group personnel.
- Coordinate implementation of the DRP strategies identified in the CAP.
- Coordinate any resource allocation conflicts among the associated teams. Collect and centrally manage resource acquisition requests, and coordinate all interfaces with the support groups on behalf of the teams.
- Coordinate the recovery of all essential operations, providing direction and guidance where required. Specific business recovery activities are contained within the respective team recovery plans.

When an incident occurs, the Management Team evaluates which response and recovery actions should be invoked and activates the corresponding recovery teams. Based on the incident, it may be necessary to request the Corporate Incident Commander to activate the corporate incident management team and support functions.

The Management Team consists of the Incident Commander, Recovery Coordinator, Recovery Team Leaders, and additional personnel as necessary. Specific representatives from the various support functions will participate in Management Team briefings and will provide support to the recovery. The Management Team is responsible for the following:

- Notification of the Corporate Incident Commander, at the corporate headquarters in St. Louis
- Assembling the consumers of the Management Team or their alternates

- Performing damage assessment to determine the severity of the incident
- Developing a CAP to provide an efficient response to the incident
- Providing on going support to the individual recovery teams as they perform their recovery procedures
- Providing and updating status to Executive Management
- Directing and coordinating the salvage, restoration, and return to the home facilities
- Ensuring the ongoing maintenance and testing of the recovery plans

The Incident Commander activates the affected team(s) following a disaster declaration.

3.4. Corporate Headquarters Impact

The Corporate Incident Management Team determines which pre-planned strategies will be used to react to the specific incident, based on the particular incident circumstances. In the event that an incident affects the data processing function for a period expected to exceed 48 hours, Centene will activate the DRP.

The Team Leaders, Disaster Recovery Coordinator and the Incident Commander will assemble in the Crisis Management Center. The location of the Crisis Management Center will be selected at the time of the incident from the Strategic Sites Report in the Business Continuity Plan. The central recovery strategy for Corporate Headquarters utilizes alternate workspace at a SunGard Recovery Services facility (i.e., St. Louis, Philadelphia, Chicago, etc.) recovery center to recover business functionality.

Network connectivity will be reestablished to the field office facilities using the SunGard network.

Once the decision to declare a disaster has been made, designated Centene recovery team personnel will be notified. The recovery teams will begin retrieving backup information, assessing damage and alerting key contacts.

3.5. Field Office Recovery

The Incident Management Team, in coordination with the Corporate Incident Management Team, determines which pre-planned strategies will be used to react to the specific incident, based on the particular incident circumstances. In the event that an incident affects the data processing function for a period expected to exceed 48 hours or phones for over 8 hours, the affected field office will activate the DRP.

In coordination with the Corporate Incident Management Team, the Field Office Team Leaders, Disaster Recovery Coordinator, and the Incident Commander will assemble in the Crisis Management Center. The location of the Crisis Management Center will be selected at the time of the incident from the Strategic Sites Report in the Reports section of this plan.

- The first business day phones will be rerouted to an alternate Centene facility, such as NurseWise.

- The recovery facility will continue to take messages until the field office's staff can take calls. The Facilities Office Support department will acquire adequate workspace locally to restore minimum services.
- The recovery facility must include provisions for staff to simultaneously access the automated systems and a voice line.
- The teams will relocate to the local recovery facility.
- A bank of phones will be allocated to take inbound calls. Phones will be rerouted to the recovery site. Alternate phones will be utilized to make outbound calls to ensure maximum availability of inbound lines.
- If adequate facility resources cannot be acquired locally in a timely manner, recovery will occur at Farmington, Missouri. Staff traveling to Farmington will be based on recovery requirements and staff availability.

To provide support to the recovery of Centene facilities outside of Corporate Headquarters, the Incident Management Team, and any other Corporate Recovery Teams necessary, will be activated to provide consultation and support to the recovery.

Once the decision to declare a disaster has been made designated Centene recovery team personnel will be notified. The recovery teams will begin retrieving backup information, assessing damage, and alerting key contacts. This potentially includes the Information Systems Team.

3.6. Incident Commander Responsibilities

The Incident Commander maintains a checklist to follow to ensure all appropriate events are initiated. Below is a sample checklist:

EVENT	SECTION REFERENCE	COMMENTS	✓
Incident Occurrence			
Initial Notification			
Plan Activation	Activation Process		
First Alert	Management Team 1st Alert Notification Summary		
Management Team Activation	Activate Management Team		
Alert Key vendors	Activate Team Leaders SunGard Disaster Alert Procedures		
Notify Internal Contacts	Activate Team Leaders		

EVENT	SECTION REFERENCE	COMMENTS	✓
Preliminary Activities			
Initiate Recovery Documentation	Maintain Recovery Related Record Keeping		
Preliminary Assessment	Preliminary Incident Assessment Meeting		
Establish Crisis Management Center	Establish the Crisis Management Center (Recovery Coordinator)		
Establish Calling Team	Establish the Crisis Management Center (Recovery Coordinator)		
Establish contact with internal Departments for recovery effort Support	Support Functions		
Assemble Management Team			
Assemble	Preliminary Incident Assessment Meeting		
Initial Briefing	Preliminary Incident Assessment Meeting		
Damage Assessment			
Determine Assessment Members	Conduct Damage Assessment Inspection		
Determine Access Procedures	Conduct Damage Assessment Inspection		
Brief Assessment Team	Conduct Damage Assessment Inspection		

EVENT	SECTION REFERENCE	COMMENTS	✓
Brief Management Team			
Present Results of Assessment	Conduct Damage Assessment Inspection		
Develop Consolidated Action Plan			
Develop Recovery Recommendation	Develop Recovery Recommendation		
Develop Contact Information	Organization Assignment List Personnel Location Control Form		
Can Recovery be Accomplished at the Home Site within the MAOD?	This question is to be answered as a result of developing the CAP at the mandatory decision time.		
If the answer to the above question is “no” or “not sure” a disaster is to be declared	Review & Finalize Consolidated Action Plan		
Initiate Disaster Declaration	Authorize Team Recovery Plan Activation		
Activate Recovery Teams	Team Activation & Disaster Declaration Procedures SunGard Disaster Declaration Procedures		
Provide ongoing support to the Individual Recovery Teams	Incident Commander’s Ongoing Responsibilities		
Assign staff to Salvage and Restoration Team	Site Restoration Overview		
Oversee Planning for Salvage & Restoration of the home site	Record and Equipment Salvage		

EVENT	SECTION REFERENCE	COMMENTS	✓
Oversee planning for, & the move back, to the home site	Plan Return Procedures		

The Incident Commander also retains ongoing responsibilities until the return to the home site:

- Determine timing for status updates to Executive Management
- Coordinate status updates from individual recovery teams with the Recovery Coordinator
- Coordinate continuing effort to locate and activate consumers of recovery team with the Recovery Coordinator
- Provide status updates to Executive Management
- Resolve any issues from recovery teams
- Identify membership of the Salvage and Restoration Team
- Coordinate efforts of the Salvage and Restoration Team
- Oversee planning for return to the home site
- Review status of unresolved problems as recovery is accomplished and after recovery is complete
- Monitor adherence to company policies during recovery
- Monitor hours worked and working conditions of recovery teams

3.7. Information Systems Team Responsibilities

In the event that an incident affects the critical automated systems, for a period expected to exceed 72-hours, Centene will activate the MIS DRP. The Recovery Point Objective for data restoration is one workday (24-hours). This is to minimize data lost from the automated systems.

The MIS Team Leader maintains communication with the Incident Commander to provide status updates and coordinate activities as needed.

Responsibilities of the MIS Team include:

- Provide support to the end users during a recovery effort
- Provide support the Claims and Plan Offices if they suffer a serious incident
- Information Systems-
- HP 9000
- AMISYS
- Supporting Infrastructure for the HP 9000
- Off-site Storage Tapes
- Serve as the liaison between all recovery teams and the off site storage provider
- Information Technology-
- Windows Servers:

- NT Servers
- Win 2000 Servers

3.8. Facility

Key business units will recover critical functionality at an alternate Centene facility that has access to phones and the automated systems. Based on the timing of the event, it may be necessary to recover at SunGard's Hotsite and to utilize a SunGard business recovery center. Alternatively, based on the event and its timing, it may be advantageous to utilize the mobile option for equipment and workspace. Based on the event, and proximity to alternate facilities, the Incident Management Team will determine the appropriate recovery option.

- **Hotsite:** In the event a disaster affects the critical automated systems, Centene will recover the affected systems at a SunGard Recovery Services (SRS) facility. The SRS Chicago MegaCenter is the designated facility based on equipment availability at the preferred recovery site.
- **Mobile Option:** Based on the incident and timing, Centene has the option to request SunGard to mobilize equipment and deliver it to a Centene facility. Prior to utilizing the mobile option confirm that the equipment on the mobile contract will meet Centene's need and that it is appropriate for the location. Refer to the SunGard Recovery Services Contract section, to identify equipment that can be transported to Centene's facility.

3.9. Systems

Data Network (WAN):

Engineers will establish connectivity from the SunGard recovery site to Centene facilities using on-demand data communications lines that have been established between the hotsite and Centene facilities.

Voice Network:

- **Centene St. Louis** - Critical "800" phone lines will be redirected to phone number(s) that will be determined at the time of the event. Redundant equipment at the Distribution Center will be utilized to maintain services for Denver, Festus, and Washington D.C. The local phone carrier will be requested to redirect critical direct dial phones to alternate phone numbers that are identified in the Telecomm report in the Logistics Team Plan
- **Remote Business Entities** - Facilities that lose voice services for a period expected to be longer than 8-hours will relocate to an alternate facility with phone and systems access. The Corporate office will redirect critical phones to the alternate facility and place a message on the other lines directing the caller to call an alternate number.

Equipment Acquisition:

The Incident Commander and/or the Executive Management Team must approve acquisition of recovery equipment that exceeds the standard purchasing authority of the recovery staff.

3.10. Disaster Recovery Plan/Business Continuity Plan Testing

The Disaster Recover Plan / Business Continuity Plan is scheduled to be tested in October 2004. Upon request, we would be pleased to share the results of this testing with ADHS/DBHS.

We are also in the process of building a back-up processing center in Montana. This facility will be in addition to and complementary with our existing centers located throughout the country. This facility will be integrated fully with Centene's existing processing facilities, enabling employees in different locations to manage data simultaneously, as well as provide a geographic diversity to further enhance redundancy objectives.

i. System Security and Audit Trail

1. Overview

Centene holds system security as a high priority and continues to support system security actions designed to implement measures that are in line with state, HIPAA and internal requirements. No hard-copy patient records are kept at any location, meaning all patient records are stored in electronic form only. This electronic data is highly secure on database servers and through controlled and managed network access. Furthermore, physical security systems of the brick-and-mortar office ensure controlled access through the use of electronic security pads that only unlock based on a user's security access coded into a magnetic swipe card. Systems allow for routine and as needed monitoring by supervisors as appropriate. These various measures are outlined and described in further detail in the sections below.

2. Firewall

Internet security was outlined in Section D - Network Configuration and Architecture. Please refer to that section for the description and diagram of our firewall configuration.

3. Encryption Technologies

PLEASE NOTE THAT THIS SECTION AND DIAGRAM ARE CONFIDENTIAL AND THUS WERE DELETED.

4. HIPAA Security Processes

Centene Corporation's current and planned procedures and compliance processes are designed to assure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- CBH and Centene take the privacy of our consumers' Protected Health Information (PHI) very seriously. Accordingly, we have had HIPAA compliant procedures in place since April 2003. To comply with the requirements of the HIPAA privacy regulations, we conducted a Gap analysis of current operations. All Gaps that were identified were remediated and policies and procedures were implemented to ensure compliance. These privacy policies and procedures have been published on the Company's Intranet site for all employees to reference. In addition:
- All workforce consumers were trained on the implemented policies and procedures.
- The training was performed by functional department and attendance of this training was documented.
- All new employees are required to participate in computer-based HIPAA Privacy training.

Furthermore, the 2004 Compliance Training contained a HIPAA Privacy refresher to remind employees of our Privacy Practices. Modifications to privacy practices are made when the Office for Civil Rights releases any pertinent guidance.

We have the ability to receive and generate standard transactions required by HIPAA. requirements and have implemented the standard code sets required by HIPAA to populate the transactions.

From a security prospective, a Gap Analysis based on the proposed HIPAA Security regulations was performed in 2002. This Gap Analysis was updated when the final Security regulations were released in February of 2003. We are currently working to remediate the gaps identified in the assessment. For example, we are actively investigating Single Sign On technology as well as various security vendors' network security products. In addition, we have tested several encryption applications for the secure transmission of electronic PHI.

The 2004 Compliance Training contained a HIPAA Security primer, covering subjects such as: strong password selection, workstation security, incident reporting, and viruses and malicious software.

Centene also provides on-going HIPAA Security workforce training and monthly email security reminders to the entire organization. Presently, we are implementing Role Base Access Control (RBAC) for both application and network access. The RBAC scheme employs a limited access privileges approach and ensures segregation of duties to reduce the risk of fraud or other possible malicious activities. We currently use SSL with 128-bit encryption on web-based services along with login IDs and passwords.

From an implementation perspective, we are aggressively addressing all requirements with HIPAA compliant solutions and will continue to implement all applicable HIPAA addressable security standards.

Role-Based Access Control (RBAC)

One of the first areas addressed as part of the HIPAA Security implementation process is employees' access to electronic consumer information. To satisfy the access control requirements of the Security Regulations, we have begun to review access to all applications containing consumer information. Standard information system access profiles are created by job description. Each of these profiles reflects the appropriate access to consumer information needed to perform the job responsibilities of that position. Depending on an employee's title, his/her access to consumer information may be expanded, significantly limited or not changed at all. In addition, access to information that is not included in a standard security profile requires the

approval and sign-off of a security official and if applicable, the functional area corporate vice president.

In order to implement RBAC, department supervisors and/or managers define the functions and access rights of employees to applications. This includes: defining the roles, establishing what authorization the roles should be entitled, and assigning employees to roles accordingly.

Role-Based Security (RBS) is a means of implementing an authorization mechanism which has the potential to substantially reduce Centene's administrative cost and reduces our security vulnerabilities. Enterprise RBS addresses the problem of maintaining authorizations within our large growing environment. RBS can better be described as RBAC. Authorization is the process through which a person is granted permission to invoke behavior, see, create, delete or update data, for one or more systems. Setting up new users and assigning authorizations are a system-by-system administrative task. This becomes a challenge as the number of systems and users becomes large, or the turnover in users becomes high. Furthermore, there is an inherent security risk in this approach; since the authorizations for a given user are dispersed across multiple systems; it becomes difficult to determine which authorizations a given user actually has.

RBS addresses security risk problems by defining an employee's access rights in a role (employees' job functions/responsibilities), thus lessening the chances of employees having unnecessary access to information. Employees' positions have sets of responsibilities, and can consequently be described with a collection of roles. Our initial effort at each location will be defining the roles, which is the most significant aspect of implementing role-based security.

With defined roles, we then associate users with their roles, and the roles with authorizations. This approach enables easier addition and removal of authorizations from users. Security changes are made to the roles versus the individuals. Associating authorizations directly with users is considered an exception, which complicates the overall goal of structured granting of authorizations.

As RBAC implementation continues across all areas of the organization:

- Granting employees' access rights will become a simple matter of associating a new user with the roles defined for the job position
- Removing security access rights to employees leaving the company can be as simple as deleting a user
- Centene will eventually have a single, explicit definition of what a user can do in our systems, thereby eliminating redundant administration and reducing the possibility for security failures in this area. This provides for correct identification and enforces separation of incompatible duties, where a user should not be a member of two roles simultaneously. For example, a single user should not have the role for authorizing a payment and the role for submitting a payment.

NOTE: The AMISYS role based security access templates are currently being tested in our Claims Processing Office. We are currently rolling this out throughout the organization.

5. Project Plan Template for Implementing Role-Based Security

The following list outlines tasks performed to implement a new area/functional group in the RBAC environment:

Location Information Access Management (AMISYS & MACESS)
[RBAC Goal: Segregation of Duties]

Determine Criteria for Establishing Access	Determine the person(s) with the responsibility of consistently requesting access rights to others: Identify the managers with access granting authority and the IS contact that communicates the request; Request and collect access rights per position information from managers Structure Employees Access Groups/Roles Utilizing Role-based access techniques (by job or by other appropriate means): Human Resources (HR) verifies the existing or creates a list of employees

	along with their job descriptions Security obtains a list of all job descriptions and system applications at these locations Department Manager (DM) creates a generic list of required software applications for each job description provided by HR Security along with DM assistance identifies all secure software applications at the location (applications or network access that require authentication) Identify the security administrator and the location of user credentials (userid/password) for each application that requires credentials for access
Determine Who Should Be Authorized to Utilized AMYSIS/MACESS Information Systems	Based on the information provided by DM identify discrepancies between the required access and the access presently granted Discuss with DM to evaluate/address any discrepancies regarding employee access to applications Trainers will provide training to the locations security staff on routine screens accessed by each specific job functions/titles
Test RBAC on Test Application Systems	Create roll back plan in case a fatal error or application shut down occurs Implement defined roles by adding/creating role based templates in application test systems Utilizing application testers, test role based access control by verifying each role has sufficient access rights so that employees in those roles can perform their job functions Test the procedure for requesting and granting rights is efficient and effective, minimizing the risk of inappropriate or insufficient granting of rights RBAC access templates, policies and procedures accordingly, removing any errors or inefficiencies discovered during testing Security creates and communicates to DM and department staff the written access rights policy; formal authorization from the appropriate authority will be required before granting access to protected healthcare information
Implement RBAC on Production Application Systems	Copy RBAC access templates from test system to production application systems Coordinate and schedule with DM's implementation of new role based access controls in production systems Implement RBAC on production systems suspending/turning off individual access rights not associated with RBAC group on production applications RBAC access templates, policies and procedures accordingly, removing any errors or inefficiencies discovered during production implementation
Monitor and Communicate Security Measures Related to Access Controls	Notify DM of RBAC implementation in production systems and provide/explain roll back plan Create a procedure to randomly audit and monitor access standards to ensure they are being followed Coordinate with other existing management operational and technical controls concerning application RBAC monitoring Update and review policies and procedures standards which include maintenance and review of audit trails, identification and authentication of users, and physical access controls

6. Sample Template of Role-Based Access Control

RBAC increases security overall, especially in the segregation of duties area. For example, the position of State Specialist requires access to setup providers and the position of Claims Analyst requires access to process claims. Employees associated with the State Specialist security role would never be included in the Claims Analyst security role and vice versa. The separation of the security roles virtually eliminates the risk of an employee setting up a fraudulent provider account and processing a claim against the account, which if allowed could possibly go unnoticed for some time before randomly being selected in an audit.

7. Security Administration for Individual Users

All individual system's security change requests are managed through a security authorization and implementation process. This process includes changes to security for existing employees, new employees and separated employees.

For employment separation circumstances, the HR site person notifies the Centene Corporate HelpDesk at least two days prior to a planned employment separation, or immediately by phone if the employment separation is not planned.

All separated employees security changes are implemented on a priority basis. All other requests are submitted to the Help Desk at least three (3) business days prior to the date required.

Security Request Forms: A detailed Security Request Form must be completed and signed by both the Department Manager and the IS Liaison/Office Manager. It is then processed as follows:

- Department Managers submit the security request forms to the IS Liaison or the Office Manager at his/her location.
- The IS Liaison or Office Service Manager then submits the forms to the Helpdesk.
- When IT has completed the requested security access, IT will contact the IS Liaison with log-in information on a new user notification form via email.
- When applicable, login IDs will be supplied by IT. The user is required to change passwords upon the first login.

Until role-based access control is fully functional for all roles within the organization, the Security Request Form provides the detailed instructions under which individual security is granted or removed. The Security Request Form_instructions are detailed below to illustrate the process followed and level of detail needed to ensure secure systems. Information required includes:

Date Submitted	Required for the date that the form is routed to the Help Desk. This field requires the following format: mo/dd/yy
Effective Date	Required for the date the security additions/modifications are to be completed. This date will be at least three days after submission date. This field requires the following format: mo/dd/yy
Reason for Request	Required so that the Helpdesk staff can immediately access the needs of the user. There are three options: new employee, current employee, and terminated employee.
General Information	To be completed by the requestor who is requesting the addition/modification of network, AMISYS, and telephone security
Last/First Name	Correct spelling of the staff member's first and last name

Department/Location	Contains a drop down list of all departments/locations
Position/Title	Used to help determine the type of access that is needed
New Position/Title	Only required when there has been a change in position/title for an existing employee
Permanent Employee	Needs to be checked for all permanent hires
Temp. Employee	Needs to be checked for all temporary hires
End Date	Last day of employment for the temporary hire in the following format: mo/dd/yy. Required field for temp staff members
Telephone Access	Used for staff members that are in need of a telephone, voice mail, and/or Agent ID setups or modifications
Extension	Used in cases where the phone extension is known to complete the set up. If an Agent-ID is necessary, the department to which the staff member needs to be added must also be entered
Voice Mail required	Drop down list with Yes or No choices
Agent ID required	Drop down list with Yes or No choices. Need to select from the list whether or not an Agent ID is required for the staff member
Agent ID Dept.	Used only if an Agent ID is necessary
Network Access	• A table where specific network access is noted. Some examples of information required in this field are: • If a home directory/folder is needed • If an email account is needed • If a staff member has access to department-shared folder • If a specific folder is needed other than the department share • If network access removal is needed
AMISYS Access	A text box for specifying whether AMISYS setup is required and for what account. Also used for changes and for removing existing access to AMISYS that is no longer necessary
Additional Software needed	• A text box for specifying any software that is necessary for the staff member to do his/her job functions. A General setup includes: • Minisoft (AMISYS) • Microsoft Outlook • Microsoft Office products (Word, Excel, Access, PowerPoint) • Examples of software that needs to be included to the field are: CCMS, MACESS, Microsoft Project and Visio etc. Justification is added to the Comments field for additional software requests. The requested software will only be added if the necessity is there for job functionality.
Comments	Used for any additional information that is necessary for the security setup of the staff member. Also used for the justification for additional software and hardware needed.

Signatures	• Forms should be routed to the Help Desk via e-mail from the Manager through the IS Liaison thus creating an electronic signature. AMISYS security requests are to be sent to an IT Security Specialist for approval prior to going to the helpdesk. If the Security Access request form is received from someone other than management, the form will be returned until proper authorization is received.

8. Systems Policies for End Users

All employees are required to follow and agree to the following systems policies as a condition of employment:

- **Passwords**. All users on a PC Network or the HP systems will be required to have a password. Users will be forced to change their passwords periodically. Passwords or access procedures ARE NOT to be written down or otherwise displayed. Passwords ARE NOT to be shared with others. Under NO circumstances are these security policies to be bypassed. Repeat offenders will be reported and may be locked out of the systems.
- **Logging Off**. PCs/terminals MUST be logged off when left unattended. This includes those times when an employee is leaving his/her desk for only a few minutes. All terminals and PC monitors should be turned off overnight. Repeat offenders will be reported to senior management and may be locked out of the systems.
- **Software**. ALL software from outside sources will be cleared through the IT Department before it is installed or used on company-owned hardware. NO game software of any type is permitted on any system. ANYONE caught playing games on company equipment while on company time will be subject to severe disciplinary actions. There will be NO exceptions.
- **Company Software**. Under no circumstances is company-owned software to be removed or copied from any system.
- **Hardware**. Company-owned computer equipment and peripherals may not be moved without prior authorization from IT. No personally-owned computers or peripherals are to be used on the premises without prior approval from IT. Additionally, no user may connect personal equipment to company equipment at any time.
- **Isolated Power**. The network systems and HP terminals are plugged into special, isolated ground power outlets or power isolation strips. Nothing else is to be plugged in to these outlets at any time. If the PC or terminal is plugged into a power strip, then nothing else is to be plugged into the same power strip. Electrical items found to be plugged in to these outlets will be unplugged; repeat offenders will be reported to senior management and will have their items confiscated by IT.
- **Access Phone Numbers**. Dial-in system access phone numbers are to be kept in the strictest confidence. Employees are instructed that if anyone requests their access number, they are to be referred to IT.
- **Backups**. The IT Department is responsible for maintaining full network backups ONLY. Individuals using local hard drives are responsible for their own backups. Local hard drives are to be used for temporary swap files and performance-dependent software applications only. Documents SHOULD NOT be kept on employees' local hard drives.

9. Protection from Malicious Software

Centene maintains an incident response plan in addition to virus scanning software that are both part of the overall solution to guard against malicious software. Users are instructed to perform

the following steps if they discover a virus or other malicious activity at their workstation such as an unidentified or strange file received through email:

1. Contact a system administrator or help desk.

- Users should not: Open the file or attempt to remedy/repair the malicious activity
- Users should not: Install any personal software or non-business related software from the Internet in an attempt to remedy the problem
- Users should: Immediately contact the help desk, system administrator, or their supervisor when unable to obtain assistance from a systems support staff member

2. Upon identification of a virus, the system will be quarantined for proper remediation.

3. Centene will update its virus definitions every 30 minutes to ensure the most up-to-date protection is provided.

10. Log-In Monitoring

Secured system administrators routinely perform maintenance or check audit/log files to ensure unauthorized log-in attempts have not been occurring. System administrators maintain an incident reporting file providing the date, time, and comments regarding any unauthorized attempts. Users are expected to report to the help desk (ext. 25244) or system administrator any suspicious activity such as: leaving their desk and returning to find that he/she has been locked out or cannot login in the morning, noticing that a different username has been entered into the log-in box, or remote access has been activated on the system without his/her knowledge (i.e. application being executed, mouse movement, etc. without user control).

11. Employee Training on Security Processes

In addition to on-going HIPAA Security workforce training and monthly email security reminders, Centene plans to implement a formal training program to comply with Standards for Security of Protected Health Information.

All persons considered part of the workforce of the Corporation will be trained on the policies and procedures regarding applicable laws and regulations regarding the security of individual health information.

Initial training will occur by April 20, 2005. The training will be incorporated into new hire orientation for all new employees. New employees will receive the training as soon as practicable following their date of hire, upon job function changes if necessary and when policies and/or procedures change. Training will be incorporated into the yearly compliance training received by all employees.

The Corporation will document that the training received by the workforce. Documentation regarding training for the Corporation's workforce will be retained for a period of at least **six** years from the date of its creation or the date when it last was in effect, whichever is later.

Training will be conducted by the Security Officer.

12. Security Audits

Centene has the ability to provide security audit data to ADBH/DBHS on an as needed basis. Audits can be performed on the specific applications on an as needed basis to include AMISYS and its various sub-systems, user network access, building security including the data center. AMISYS audit capabilities are outlined below.

AMISYS Audit capabilities:

All transaction-related and date-sensitive records throughout the AMISYS system (e.g., consumer records, provider contract records, Encounter/Claims records) are affixed automatically by AMISYS with two audit-related data items:

- A 'date stamp' in the form of a Trans date, which represents the date the record was last changed or 'touched'
- An Operator Number (Op#) which indicates the person or program responsible for that change
- Depending on the nature of the record, it may also have an associated Trans Code representing the 'type' of change that was made, for example, a consumer record with a Trans Code equal to 'SP' indicating that the date span has been changed. Trans Codes are subsystem-specific as the types of changes and/or updating that effect records vary amongst the subsystems.

The Trans dates, Operator Numbers and Trans Codes are housed in the database and displayed on the corresponding record screen making it easy to determine the most recent change affecting a given record.

AMISYS features a comprehensive Claims Audit Function with definable parameters enabled to allow for tracking of all changes to a claim or service in the transaction system. A unique audit record is created and saved in the transaction (HEALTH) database of AMISYS for each modification to a service or claim including adjustments, providing a complete historical accounting for every change, manual or programmatic, to a service or claim.

The associated audit records for a claim or service are retained in the database for 90 days after resolution (payment or denial) of the claim and may be readily accessed and used for auditing, tracking and reporting purposes.

Date Span Logic exists for All Records critical to Claims adjudication, Processing and Payment. Group, Division and Consumer records have associated date-spans (Consumer spans) which house such critical and process-sensitive data as:

- The line of business
- Effective and end dates
- Benefit Package
- Billing Method
- Primary Care Physician
- Employee Status

Data Span Logic allows the transaction system to access and utilize processing parameters for a period of time specific to a date of service, accommodating current and retroactive processing. Historical records are updated and retained in the database with each change (including voids) to a data item in the Group, Division and Member spans and may also be accessed via on-line action commands or through the Inquiry Subsystem.

Provider Affiliation Records, which equate to the contractual agreement within AMISYS, also include date-spans enabling the plan to store current as well as historical data relating to:

- Provider Status
- Line of business
- Tax Identification Numbers
- Medicaid Numbers
- Reimbursement methodologies including associated fee schedules
- Date spans ensure the appropriate processing of transactions, either current or retroactive, by utilizing only the data relevant at the point in time associated with the date of service.

j. Information Systems Data Mapping

1. Overview

Centene's MIS Department complies with the certificate of coverage and data specification reporting requirements related to HIPAA. To comply with these requirements, the department utilizes translation software, EC Map, to map, translate and compliance check inbound and outbound HIPAA transactions. Centene has adopted the National Electronic Data Interchange Transaction Set Implementation Guides (IG). While Centene has developed its own technical companion guides, covering certain of these transactions, to assist application developers during the implementation process, the information contained in our Companion Guides is only intended to supplement the adopted IGs The Centene Companion Guide is never intended to modify, contradict, or interpret the rules established in HIPAA or contained in the IG's.

As indicated in section E, Ability to Provide Secure Electronic Data Interface, we have also received certifications that our 837I and 837P files are HIPAA compliant.

Centene has the capability to store data elements that are not currently captured, stored or used. We would store the necessary data elements in an external (external from AMISYS) data set with ability to access later.

This section provides general transmission instructions and processes, as well as the specific data maps for the 834 Intake and Closure, 837I (Institutional Claim) and 837P (Professional Claim), NCPDP (Drug Claim), Demographic and Other transactions, where applicable. In addition, the requirements for establishing electronic data exchange capabilities with GREABHA are provided.

2. General Instructions and Processes

2.1. Basic Technical Information

The following list includes some basic technical information:

- Lower case characters on inbound transactions are converted to uppercase on outbound transactions
- The following delimiters are used for all outbound transactions:

*	(Asterisk)	=	Data element separator
:	(Colon)	=	Sub element separator
~	(Tilde)	=	Segment separator

- Interactive transaction must contain only one request
- All monetary amounts and quantity fields have explicit decimals. The decimal point always appears in the character stream if the decimal point is at any place other than the right end. If the value is an integer, with the decimal point at the right end, the decimal point should be omitted. See the IG for additional clarification. Centene is referred to as Centene in applicable Submitter and Receiver segments.
- The TA1 – Interchange Acknowledgement, is not used.

- The 997 – Functional Acknowledgement, is generated in response to all inbound batch transactions.
- The 997 – Functional Acknowledgement, is expected in response to all outbound batch transactions created by Centene.
- Required data elements considered non-critical to Centene processing that must be returned on outbound transactions, such as member's birth date, are returned as they appear on the Centene files.
- If one item within a functional group is non-compliant, the entire transaction, ST-SE, is rejected.
- Data elements required by the IG, but not used by Centene can be gap-filled with any valid value to avoid compliance errors.

2.2. Method of Transmission

Centene has secure options available for exchanging data electronically. All transactions will be submitted in a batch mode. There are two methods of sending and receiving electronic transactions with Centene. Those two methods are:

- Centene Bulletin Board System (BBS)
- Trading Partner's BBS or FTP site

2.3. Data Flow

Functional Acknowledgement

For each batch transaction received, Centene will return a 997 – Functional Acknowledgement. This file acknowledges the receipt of the file and reports any data compliance issues. Centene also expects to receive file receipt confirmation when the trading partner receives any outbound batch transaction. The available methods of confirmation are: 997 – Functional Acknowledgement transaction, email, or telephone.

The software used by Centene is Sybase's EC MAP with a HIPAA toolkit extension. Sybase's method for creating a 997 acknowledgement is to run data through a compliance map. The compliance map is defined to validate the EDI against the complete standard transaction set definition or to validate EDI data against a specific subset of the standard transaction.

Centene implemented the standard HIPAA compliance maps created by Sybase without modifications. If any part of the transaction from the ISA to IEA does not pass Compliance, the entire file will not be processed and will need to be fixed by the sender and resent.

Audit Report

We have created an Audit Report for any encounter transaction (837I and 837P) received. This is not a HIPAA-mandated report; however it summarizes the number of claims received and any claims that were rejected due to invalid information. Any encounter that has been rejected and is acknowledge on this report, must be fixed and resent either electronically via an 837 or on paper. Those encounters that have been rejected are based on up front edits and do not pertain to our adjudication process.

The sample audit report contains the following fields:

Process Date	6 characters	Date Claims Processed (CCMMDD)
Claim Number	12 characters	Centene Claim Number

Member	12 characters	Centene Member Number
Amt Billed	10 characters	Billed Amount for Claim 9(07)v99
Status	6 characters	ACCEPT or INVALD
Prov Nbr	6 characters	Centene Provider Number
Mdcaid Nbr	9 characters	Provider Tax ID Number
Reason	2 characters	Reason for error if INVALD status (see below)
Serv Date	8 characters	Date of Service
Patient	17 characters	Patient ID as sent by provider

Following is the sample audit report:

PROCESS DATE	CLAIM NUMBER	MEMBER	AMT BILLED	STATUS	PROV NBR	MCAID NBR	REASON	SERV DATE	PATIENT ID
010604	011550031280	11111111111	000005500	INVALD	232323232	2674893	06	20011110	3T12579039
010604	011550031380	22222222222	000160904	ACCEPT	200000	2674894		20011026	3T12579407
010604	011550031480	33333333333	000007700	INVALD	300009	2674895	01	20011110	3T12579042
010604	011550031580	44444444444	000014900	ACCEPT	555666	2674896		20011117	3T12579048
010604	011550031680	44444444444	000007700	ACCEPT	555666	2674896		20011117	3T12579049
010604	011550031780	44444444444	000007000	ACCEPT	555666	2674896		20011129	3T12580690
010604	011550031880	44444444444	000022700	ACCEPT	555666	2674896	17	20011129	3T12580691
010604	011550031980	44444444444	000005500	ACCEPT	555666	2674896		20011117	3T12579056
010604	011550032080	44444444444	000009300	ACCEPT	555666	2674896		20011117	3T12580680
010604	011550032180	55555555555	000030700	ACCEPT	808999	2674897		20011206	3T12583224
010604	011550032280	55555555555	000036500	ACCEPT	808999	2674897		20011212	3T12583191
010604	011550032380	66666666666	000027500	ACCEPT	776776	2674898		20011206	3T12583265
010604	011550032480	77777777777	000037300	ACCEPT	220220	2674899		20011206	3T12583212
010604	011550032580	12121212121	000022800	INVALD	100000	2674893	02	20011212	3T12583199
010604	011550032680	13131313131	000110200	INVALD	999999999	2674893	08	20011209	3T12579770

***TOTAL CLAIMS ACCEPTED 00011

***TOTAL CLAIMS REJECTED 00004

Following is a listing of the error codes that may be returned on the Audit Report:

01 Invalid Mbr DOB
02 Invalid Mbr
06 Invalid Prv
07 Invalid Mbr DOB & Prv
08 Invalid Mbr & Prv
09 Mbr not valid at DOS
10 Invalid Mbr DOB; Mbr not valid at DOS
12 Prv not valid at DOS
13 Invalid Mbr DOB; Prv not valid at DOS
14 Invalid Mbr; Prv not valid at DOS
15 Mbr not valid at DOS; Invalid Prv
16 Invalid Mbr DOB; Mbr not valid at DOS; Invalid Prv
17 Invalid Diag

18 Invalid Mbr DOB; Invalid Diag
19 Invalid Mbr; Invalid Diag
21 Mbr not valid at DOS; Prv not valid at DOS
22 Invalid Mbr DOB; Mbr not valid at DOS; Prv not valid at DOS
23 Invalid Prv; Invalid Diag
24 Invalid Mbr DOB; Invalid Prv; Invalid Diag
25 Invalid Mbr; Invalid Prv; Invalid Diag
26 Mbr not valid at DOS; Invalid Diag
27 Invalid Mbr DOB; Mbr not valid at DOS; Invalid Diag
29 Prv not valid at DOS; Invalid Diag
30 Invalid Mbr DOB; Prv not valid at DOS; Invalid Diag
31 Invalid Mbr; Prv not valid at DOS; Invalid Diag
32 Mbr not valid at DOS; Prv not valid; Invalid Diag
33 Invalid Mbr DOB; Mbr not valid at DOS; Invalid Prv; Invalid Diag
34 Invalid Proc
35 Invalid Mbr DOB; Invalid Proc
36 Invalid Mbr; Invalid Proc
38 Mbr not valid at DOS; Prv not valid at DOS; Invalid Diag
39 Invalid Mbr DOB; Mbr not valid at DOS; Prv not valid at DOS; Invalid Diag
40 Invalid Prv; Invalid Proc
41 Invalid Mbr DOB, Invalid Prv; Invalid Proc
42 Invalid Mbr; Invalid Prv; Invalid Proc
43 Mbr not valid at DOS; Invalid Proc
44 Invalid Mbr DOB; Mbr not valid at DOS; Invalid Proc
46 Prv not valid at DOS; Invalid Proc
48 Invalid Mbr; Prv not valid at DOS; Invalid Proc
49 Mbr not valid at DOS; Invalid Prv; Invalid Proc
51 Invalid Diag; Invalid Proc
52 Invalid Mbr DOB; Invalid Diag; Invalid Proc
53 Invalid Mbr; Invalid Diag; Invalid Proc
57 Invalid Prv; Invalid Diag; Invalid Proc
58 Invalid Mbr DOB; Invalid Prv; Invalid Diag; Invalid Proc
59 Invalid Mbr; Invalid Prv; Invalid Diag; Invalid Proc
60 Mbr not valid at DOS; Invalid Diag; Invalid Proc
61 Invalid Mbr DOB; Mbr not valid at DOS; Invalid Diag; Invalid Proc
63 Prv not valid at DOS; Invalid Diag; Invalid Proc
64 Invalid Mbr DOB; Prv not valid at DOS; Invalid Diag; Invalid Proc
65 Invalid Mbr; Prv not valid at DOS; Invalid Diag; Invalid Proc
66 Mbr not valid at DOS; Invalid Prv; Invalid Diag; Invalid Proc
67 Invalid Mbr DOB; Mbr not valid at DOS; Invalid Prv; Invalid Diag; Invalid Proc
72 Mbr not valid at DOS; Prv not valid at DOS; Invalid Diag; Invalid Proc
73 Invalid Mbr DOB; Mbr not valid at DOS; Prv not valid at DOS; Invalid Diag; Invalid Proc

Batch Request or Inquiry Transaction

A batch request or inquiry transaction, 270, 276, 278 results in the creation of the response transaction, 271, 277 or 278 respectively. Centene will post the responses in a reasonable amount of time for the requestor to retrieve.

Other Transactions

Finally, some transactions can be submitted interactively. Centene only creates a 997 – Acknowledgement for an interactive request transaction if it fails the compliance check. Otherwise, the appropriate response transaction serves as the acknowledgement of the receipt of the transaction.

2.4. Interchange Control Structure

Data files are transmitted in an electronic envelope. The communication envelope consists of an interchange envelope and functional groups. The interchange control structure is used for inbound and outbound files. An inbound interchange control structure is the envelope that wraps all transaction data (ST-SE) sent to Centene for processing. Examples include 837, 270 and 276 transactions. An outbound interchange control structure wraps transactions that are created by Centene and returned to the requesting provider or contracted vendor. Examples of outbound transactions include 835, 271 and 277 transactions.

3. File Specific Requirements and Data Maps

3.1. 834 (Intake and Closure)

GREABHA has the capability of receiving enrollment data via the 834 HIPAA transaction. Centene has a proven track record of successfully implementing this transaction. The ASC X12N 834 (004010X095) transaction is the HIPAA-mandated transaction for submitting Centene benefit and enrollment information to Business Associates: Covered Entities and Non-Covered Entities.

One version of the 834 file will be made available by Centene which will be considered an Audit File in 834 terminology. Centene will supply a supplemental “Change” upon request. The change file will contain any member that a new member span was created. The Change file will accompany the Audit file, and will be in the same format. The Change file will be denoted by a “2” and the Audit file will be denoted by a “4”.

The Audit File will be made available based on a defined schedule. This file will contain member information on currently enrolled and active members only. Terminated members will not be provided in this file. If a member was in the previous file submitted but is not in the current file received, the expectation is that member has been terminated or placed on review.

Segment Usage

The following matrix lists all segments available to the submitted 834 transaction. Additionally, it includes a Usage column that identifies those segments, which are required, situational, or not used by Centene. A required segment element will be reported on all transactions. A situational segment may not be reported on every transaction record; however, a situational segment may be reported under certain circumstances. For example, any data in a segment that is identified in the Usage column with an X will be ignored by Centene. Other requirements for this file include:

- The maximum number of records within a single 834 Transaction is 10,000. Therefore, multiple 834 transactions may exist within one file.
- Some element values may be defined as NULL. This means that there will not be a value in this element (i.e. INS*Y*18*001**A*B**FT)

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
ST	N/A	Transaction Set Header	R
BGN	N/A	Beginning Segment	R
REF	N/A	Transaction Set Policy Number	R
DTP	N/A	File Effective Date	R
N1	1000A	Sponsor Name	R
N1	1000B	Payer	R
N1	1000C	TPA/Broker Name	X
ACT	1100C	TPA/Broker Account Information	X
INS	2000	Member Level Detail	R
REF	2000	Subscriber Number	R
REF	2000	Member Policy Number	R
REF	2000	Member Identification Number	S
REF	2000	Prior Coverage Months	X
DTP	2000	Member Level Dates	R
NM1	2100A	Member Name	R
PER	2100A	Member Communications Number	S
N3	2100A	Member Residence Street Address	R
N4	2100A	Member Residence City, State, Zip	R
DMG	2100A	Member Demographics	R
ICM	2100A	Member Income	X
AMT	2100A	Member Policy Amounts	X
HLH	2100A	Member Health Information	X
LUI	2100A	Member Language	X
NM1	2100B	Incorrect Member Name	X
DMG	2100B	Incorrect Member Demographics	X
NM1	2100C	Member Mailing Address	X
N3	2100C	Member Mail Street Address	X
N4	2100C	Member Mail City, State, Zip	X
NM1	2100D	Member Employer	X
PER	2100D	Member Employer Communications Numbers	X
N3	2100D	Member Employer Street Address	X
N4	2100D	Member Employer City, State, Zip	X
NM1	2100E	Member School	X
PER	2100E	Member School Communications Numbers	X
N3	2100E	Member School Street Address	X
N4	2100E	Member School City, State, Zip	X
NM1	2100F	Custodial Parent	X
PER	2100F	Custodial Parent Communications Numbers	X
N3	2100F	Custodial Parent Street Address	X
N4	2100F	Custodial Parent City, State, Zip	X
NM1	2100G	Responsible Person	X
PER	2100G	Responsible Person Communications Numbers	X
N3	2100G	Responsible Person Street Address	X
N4	2100G	Responsible Person City, State, Zip	X
DSB	2200	Disability Information	X
DTP	2200	Disability Eligibility Dates	X
HD	2300	Health Coverage	R

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
DTP	2300	Health Coverage Dates	S
AMT	2300	Health Coverage Policy	X
REF	2300	Health Coverage Policy Number	X
IDC	2300	Identification Card	X
LX	2310	Provider Information	R
NM1	2310	Provider Name	R
N4	2310	Provider City, State, Zip	X
PER	2310	Provider Communications Number	X
PLA	2310	PCP Change Reason	X
COB	2320	Coordination of Benefits	X
REF	2320	Additional Coordination of Benefits Identifiers	X
N1	2320	Other Insurance Company Name	X
DTP	2320	Coordination of Benefits Eligibility Dates	X
SE	N/A	Transaction Set Trailer	R

1 ***Data Map***

2 Following is the data map for the 834 file specific to ADHS/DBHS:

ADHS/DBHS					Centene		
Segment ID	**Loop**	**Segment Name**	**Usage**		**Segment ID**	**Loop**	**Segment Name**
BGN02	N/A	Reference Identifier	R		BGN02	N/A	Reference Identifier - conditional store variable
INS03	2000	Maintenance Type Code	R		INS03	2000	Maintenance Type Code - conditional store variable (1)
INS04	2000	Maintenance Reason Code	S		INS04	2000	Maintenance Reason Code - conditional store variable (195)
DTP01	2000	Date/Time Qualifier "356" and "357"	R		DTP01	2000	Date /Time Qualifier - conditional store variable
DTP03	2000	Date Time Period	R		DTP03	2000	Date Time Period (175-182)(183-190)
REF01	2000	Reference Identification Qualifier "0F"	R		REF01	2000	Subscriber Number Qualifier "0F" -conditional store variable
REF02	2000	Subscriber Number	R		REF02	2000	Recipient ID number (12-23)
NM103	2100A	Member Name , Last	R		NM103 INS	2100A	Recipient Last Name (24-38)
NM104	2100A	Member Name , First	R		NM104 INS	2100A	Recipient First Name (39-51)
NM105	2100A	Member Name Middle initial	S		NM105 INS	2100A	Recipient Middle Name (52)
NM108	2100A	"34" Social Security Number	S		NM109 INS	2100 A	Recipient Social Security Number (61-69)
N301	2100A	Member Street Address Line 1	R		N3	2100A	Address Information (70-99)
N302	2100A	Member Street Address Line 2	S		N3	2100A	Address Information 2 (100-129)
N401	2100A	City	R		N401	2100A	Recipient City (130-144)
N402	2100A	State	R		N402	2100A	Recipient State (145-146)
N403	2100A	Postal Code	R		N403	2100A	Recipient Postal Code (147-155)

ADHS/DBHS					Centene		
Segment ID	Loop	Segment Name	Usage		Segment ID	Loop	Segment Name
N405	2100A	"CY" county qualifier	S		N405	2100A	"CY" county qualifier - conditional store variable
N406	2100A	Location Identification	S		N406	2100A	Recipient County Code (196-197)
DMG01	2100A	Date Time period format Qualifier "D8"	S		DMG01	2100A	Date Qualifier - conditional store variable
DMG02	2100A	Date Time Period Date of Birth	R		DMG02	2100A	Recipient Birth date (53-60)
DMG03	2100A	Gender Code	R		DMG03	2100A	Gender Code (156)
HD03	2300	Health Coverage Plan Coverage Description	R		HD03	2300	Plan Coverage Description - conditional store variable (191-192)

3.2. 837I (Institutional) and 837P (Professional)

GREABHA has the capability to receive both Institutional and Professional claim/encounter data via the 837 HIPAA transaction. The ASC X12N 837 (004010X096) transaction is the HIPAA-mandated transaction for submitting Centene benefit and enrollment information to Covered Entities and Business Associates.

One version of the 837 file will be made available by Centene which will be considered an Audit File in 834 terminology. The Audit File will be made available based on a specified. This file will contain member information on currently enrolled and active members only. Terminated members will not be provided in this file. If a member was in the previous file submitted but is not in the current file received, the expectation is that member has been terminated or placed on review.

Segment Usage

The following matrix lists all segments available to the submitted 837 transaction. Additionally, it includes a Usage column that identifies those segments, which are required, situational, or not used by Centene. A required segment element will be reported on all transactions. A situational segment may not be reported on every transaction record; however, a situational segment may be reported under certain circumstances. For example, any data in a segment that is identified in the Usage column with an X will be ignored by Centene. Other requirements for this file include:

1. The maximum number of records within a single 837 Transaction is 10,000. Therefore, multiple 837 transactions may exist within one file.

2. Some element values may be defined as NULL. This means that there will not be a value in this element (i.e. INS*Y*18*001**A*B**FT)

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
ST	N/A	Transaction Set Header	R
BHT	N/A	Beginning of Hierarchical Transaction	R
REF	N/A	Transmission Type Identification	R
NM1	1000A	Submitter Name	R
PER	1000A	Submitter EDI Contact Information	R
NM1	1000B	Receiver Name	X
HL	2000A	Billing/Pay-To Hierarchical Level	X

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
PRV	2000A	Billing/Pay-To Specialty Information	X
CUR	2000A	Foreign Currency Information	X
NM1	2010AA	Billing Provider Name	R
N3	2010AA	Billing Provider Address	R
N4	2010AA	Billing Provider City/State/Zip Code	R
REF	2010AA	Billing Provider Secondary Information	R
REF	2010AA	Credit/Debit Card Billing Information	X
PER	2010AA	Billing Provider Contact Information	R
NM1	2010AB	Pay-To Provider Name	X
N3	2010AB	Pay-To Provider Address	X
N4	2010AB	Pay-To Provider City/State/Zip Code	X
REF	2010AB	Pay-To Provider Secondary Information	X
HL	2000B	Subscriber Hierarchical Level	X
SBR	2000B	Subscriber Information	R
NM1	2010BA	Subscriber Name	R
N3	2010BA	Subscriber Address	R
N4	2010BA	Subscriber City/State/Zip Code	R
DMG	2010BA	Subscriber Demographic Information	R
REF	2010BA	Subscriber Secondary Information	X
REF	2010BA	Property and Casualty Claim Number	X
NM1	2010BB	Credit/Debit Card Account Holder Name	X
REF	2010BB	Credit/Debit Card Information	X
NM1	2010BC	Payer Name	R
N3	2010BC	Payer Address	R
N4	2010BC	Payer City/State/Zip Code	R
REF	2010BC	Payer Secondary Information	S
NM1	2010BD	Responsible Party Name	X
N3	2010BD	Responsible Party Address	X
N4	2010BD	Responsible Party City/State/Zip Code	X
HL	2000C	Patient Hierarchical Level	X
PAT	2000C	Patient Information	R
NM1	2010CA	Patient Name	S
N3	2010CA	Patient Address	S
N4	2010CA	Patient City/State/Zip Code	S
DMG	2010CA	Patient Demographic Information	S
REF	2010CA	Patient Secondary Information Number	X
REF	2010CA	Property and Casualty Claim Number	X
CLM	2300	Claim Information	R
DTP	2300	Discharge Hour	S
DTP	2300	Statement Dates	R
DTP	2300	Admission Date/Hour	S
CL1	2300	Institutional Claim Code	S
PWK	2300	Claim Supplemental Information	X
CN1	2300	Contract Information	X
AMT	2300	Payer Estimated Amount Due	R
AMT	2300	Patient Estimated Amount Due	X
AMT	2300	Patient Paid Amount	S
AMT	2300	Credit/Debit Card Maximum Amount	X
REF	2300	Adjusted Repriced Claim Number	X
REF	2300	Repriced Claim Number	X
REF	2300	Claim Identification Number for	X

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
		Clearinghouses and Other Transmission Intermediaries	
REF	2300	Document Identification Code	S
REF	2300	Original Reference Number (ICN/DCN)	S
REF	2300	Investigational Device Exemption Number	S
REF	2300	Service Authorization Exception Code	X
REF	2300	Peer Review Organization (PRO) Approval Number	X
REF	2300	Prior Authorization or Referral Number	S
REF	2300	Medical Record Number	S
REF	2300	Demonstration Project Identifier	X
K3	2300	File Information	X
NTE	2300	Claim Note	S
NTE	2300	Billing Note	S
CR6	2300	Home Health Care Information	S
CRC	2300	Home Health Functional Liabilities	S
CRC	2300	Home Health Activities Permitted	S
CRC	2300	Home Health Mental Status	S
HI	2300	Principal, Admitting, E-code, and Patient Reason for Visit Diagnosis Information	R
HI	2300	Diagnosis Related Group (DRG) Information	S
HI	2300	Other Diagnosis Information	S
HI	2300	Principal Procedure Information	S
HI	2300	Other Procedure Information	S
HI	2300	Occurrence Span Information	S
HI	2300	Occurrence Information	S
HI	2300	Value Information	S
HI	2300	Condition Information	S
HI	2300	Treatment Code Information	S
QTY	2300	Claim Quantity	S
HCP	2300	Claim Pricing/Repricing Information	X
CR7	2305	Home Health Care Plan Information	S
HSD	2305	Home Care Services Delivery	S
NM1	2310A	Attending Physician Name	S
PRV	2310A	Attending Physician Specialty Information	X
REF	2310A	Attending Physician Secondary Information	S
NM1	2310B	Operating Physician Name	S
PRV	2310B	Operating Physician Specialty Information	X
REF	2310B	Operating Physician Secondary Information	S
NM1	2310C	Other Provider Name	S
PRV	2310C	Other Provider Specialty Information	X
REF	2310C	Other Provider Secondary Information	S
NM1	2310E	Service Facility Name	X
PRV	2310E	Service Facility Specialty Information	X
N3	2310E	Service Facility Address	X
N4	2310E	Service Facility City/State/Zip Code	X
REF	2310E	Service Facility Secondary Information	X
SBR	2320	Other Subscriber Information	S
CAS	2320	Claim Level Adjustment	X
AMT	2320	Payer Prior Payment	S
AMT	2320	Coordination of Benefits (COB) Total	X

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
		Allowed Amount	
AMT	2320	Coordination of Benefits (COB) Total Submitted Charges	X
AMT	2320	Diagnosis Related Group (DRG) Outlier Amount	X
AMT	2320	Coordination of Benefits (COB) Total Medicare Paid Amount	X
AMT	2320	Medicare Paid Amount – 100%	X
AMT	2320	Medicare Paid Amount – 80%	X
AMT	2320	Coordination of Benefits (COB) Medicare A Trust Fund Paid Amount	X
AMT	2320	Coordination of Benefits (COB) Medicare B Trust Fund Paid Amount	X
AMT	2320	Coordination of Benefits (COB) Total Non-covered Amount	X
AMT	2320	Coordination of Benefits (COB) Total Denied Amount	X
DMG	2320	Other Subscriber Demographic Information	S
OI	2320	Other Insurance Coverage Information	S
MIA	2320	Medicare Inpatient Adjudication Information	X
MOA	2320	Medicare Outpatient Adjudication Information	X
NM1	2330A	Other Subscriber Name	S
N3	2330A	Other Subscriber Address	S
N4	2330A	Other Subscriber City/State/Zip Code	S
REF	2330A	Other Subscriber Secondary Information	S
NM1	2330B	Other Payer Name	S
N3	2330B	Other Payer Address	S
N4	2330B	Other Payer City/State/Zip Code	S
DTP	2330B	Claim Adjudication Date	X
REF	2330B	Other Payer Secondary Identification and Reference Number	S
REF	2330B	Other Payer Prior Authorization or Referral Number	X
NM1	2330C	Other Payer Patient Information	X
REF	2330C	Other Payer Patient Identification Number	X
NM1	2330D	Other Payer Attending Provider	X
REF	2330D	Other Payer Attending Provider Identification	X
NM1	2330E	Other Payer Operating Provider	X
REF	2330E	Other Payer Operating Provider Identification	X
NM1	2330F	Other Payer Other Provider	X
REF	2330F	Other Payer Other Provider Identification	X
NM1	2330G	Other Payer Referring Provider	X
REF	2330G	Other Payer Referring Provider Identification	X
NM1	2330H	Other Payer Service Facility Provider	X
REF	2330H	Other Payer Service Facility Provider Identification	X
LX	2400	Service Line Number	R
SV2	2400	Institutional Service Line	R
PWK	2400	Line Supplemental Information	X
DTP	2400	Service Line Date	S

Segment ID	Loop ID	Segment Name	Usage R –Required S- Situational X – Not Used
STP	2400	Assessment Date	X
AMT	2400	Service Tax Amount	X
AMT	2400	Facility Tax Amount	X
LIN	2410	Drug Identification – *New segment per addenda*	X
CTP	2410	Drug Pricing – *New segment per addenda*	X
REF	2410	Prescription Number	X
NM1	2420A	Attending Physician Name	X
REF	2420A	Attending Physician Secondary Information	X
NM1	2420B	Operating Physician Name	X
REF	2420B	Operating Physician Secondary Information	X
NM1	2420C	Other Provider Name	X
REF	2420C	Other Provider Secondary Information	X
SVD	2430	Service Line Adjudication Information	X
CAS	2430	Service Line Adjustment	X
DTP	2430	Service Line Adjudication Date	X
SE	N/A	Transaction Set Trailer	R

***Data Map* -837 Institutional file**

Following is the data map for the 837 Institutional file, specific to ADHS/DBHS:

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
ST01		Trans. Set Header - 837	R	ST01		Trans. Set Header - 837
ST02		Trans. Set Control Number - Incremented Number	R	ST02		Trans. Set Control Number - Incremented Number
BHT01		Hierarchical Structure Code - 0019	R	BHT01		Hierarchical Structure Code - 0019
BHT02		Trans. Set Purpose Code - 00	R	BHT02		Trans. Set Purpose Code - 00
BHT03		Reference Identifier	R	BHT03		Constant 1
BHT04		Date	R	BHT04		Process-Date
BHT05		Time	R	BHT05		Constant 1200
BHT06		Trans. Type Code - RP	R	BHT06		Transaction Type Code RP
REF01		Reference I.D. Qualifier - 87	R	REF01		Reference Identification Qualifier - 87
REF02		Reference Identifier - 00410X096A1	R	REF02		Reference Identifier - 00401X096A1
NM101	1000A	Entity Identifier Code - 41	R	NM101	1000A	Entity Identifier Code - 41
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name - RBHA Name	R	NM103		Submitter-Name
NM104		Name First		NM104		

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
NM105		Name Middle		NM105		
NM108		Identification Code Qualifier - 46	R	NM108		Identification Code Qualifier - 46
NM109		Identification Code - RBHA Contractor ID	R	NM109		Identification Code - 401M
PER01	1000A	Contact Function Code - IC	R	PER01	1000A	Contact Function Code - IC
PER02		Name	R	PER02		Submitter-Name
PER03		Comm. Number Qualifier - ED, EM, FX, TE	R	PER03		Comm. Number Qualifier - TE
PER04		Comm. Number	R	PER04		Submitter-Tel
PER05		Comm. Number Qualifier		PER05		
PER06		Comm Number		PER06		
PER07		Comm. Number Qualifier		PER07		
PER08		Comm. Number		PER08		
NM101	1000B	Entity Identifier Code - 40	R	NM101	1000B	Entity Identifier Code - 40
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name	R	NM103		Receiver
NM108		Identification Code Qualifier - 46	R	NM108		Identification Code Qualifier - 46
NM109		Identification Code	R	NM109		Receiver-ID
HL01	2000A	Hierarchical ID Number	R	HL01	2000A	Memory Variable HL01 Hierarchical Level Counter
HL03		Hierarchical Level Code - 20	R	HL03		Hierarchical Level Code - 20
HL04		Hierarchical Child Code - 1	R	HL04		Hierarchical Child Code - 1
NM101	2010AA	Entity Identifier Code - 85	R	NM101	2010AA	Entity Identifier Code - 85
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name	R	NM103		Prov-Name
NM108		Identification Code Qualifier - 24	R	NM108		Identification Code Qualifier - 24
NM109		Identification Code	R	NM109		Prov-EIN
N301	2010AA	Address Information	R	N301	2010AA	Prov-Addr
N302		Address Information		N302		
N401		City Name	R	N401		Prov-City

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
N402		State or Providence Code	R	N402		Prov-State
N403		Postal Code	R	N403		Prov-Zip
N404		Country Code		N404		
REF01	2010 AA	Reference Ident. Qualifier - 1D	R	REF01	2010A A	Reference Ident. Qualifier - 1D
REF02		Reference Identifier - Provider ID	R	REF02		Prov-Medicaid-NBR
NM101	2010 AB	Entity Identifier Code - 87	R	NM101	2010A B	Currently Not Mapped, New constant - 87
NM102		Entity Type Qualifier - 2	R	NM102		Currently Not Mapped, New constant - 2
NM103		Name Last / Org. Name	R	NM103		Currently Not Mapped, New field - PayToProv-Name
NM108		Identification Code Qualifier - 24	R	NM108		Currently Not Mapped, New constant - 24
NM109		Identification Code	R	NM109		Currently Not Mapped, New field, PayToProvider-EIN
N301	2010 AB	Address Information	R	N301	2010A B	Currently Not Mapped, New field, PayToProvider-Addr1
N302		Address Information		N302		
N401	2010 AB	City Name	R	N401	2010A B	Currently Not Mapped, New field, PayToProvider-City
N402		State or Providence Code	R	N402		Currently Not Mapped, New field, PayToProvider-State
N403		Postal Code	R	N403		Currently Not Mapped, New field, PayToProvider-Zip
N404		Country Code		N404		
REF01	2010 AB	Reference Ident. Qualifier - G2	R	REF01	2010A B	Currently Not Mapped, New constant- G2
REF02		Reference Identifier - Provider ID	R	REF02		Currently Not Mapped, New field - PayToProvider- ID
HL01	2000 B	Hierarchical ID Number	R	HL01	2000B	Memory Variable: HL01: Hierarchical Level Counter
HL02		Hierarchical Parent ID Num - 1	R	HL02		Hierarchical Parent ID Num - 1
HL03		Hierarchical Level Code - 22	R	HL03		Hierarchical Level Code - 22
HL04		Hierarchical Child Code - 0	R	HL04		Hierarchical Child Code - 0
SBR01	2000 B	Payer Resp. Seq. Num Code - T	R	SBR01	2000B	Payer Resp. Seq. Num Code - T
SBR02		Individual Relationship Code - 18	S	SBR02		Individual Relationship Code - 18

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
SBR03		Reference Identifier		SBR03		
SBR04		Name	S	SBR04		Insured-Grp-Name
SBR09		Claim Filing Indicator Code - MC	S	SBR09		Claim Filing Indicator Code - MC
NM101	2010 BA	Entity Identifier Code - IL	R	NM101	2010B A	Entity Identifier Code - IL
NM102		Entity Type Qualifier - 1	R	NM102		Entity Type Qualifier - 1
NM103		Name Last / Org. Name	R	NM103		Patient-Lname
NM104		Name First		NM104		
NM105		Name Middle		NM105		
NM107		Name Suffix		NM107		
NM108		Identification Code Qualifier - MI	R	NM108		Identification Code Qualifier - MI
NM109		Identification Code - Client ID	R	NM109		ID-NBR
N301	2010 BA	Address Information	R	N301	2010B A	Patient-Addr1
N302		Address Information		N302		
N401	2010 BA	City Name	R	N401	2010B A	Patient-City
N402		State or Providence Code	R	N402		Patient-State
N403		Postal Code	R	N403		Patient-Zip
N404		Country Code		N404		
DMG01	2010 BA	Date Time Period Form.Qual. - D8	R	DMG01	2010B A	Date Time Period Form.Qual. - D8
DMG02		Date Time Period - Subscriber DOB	R	DMG02		Patient-Birth
DMG03		Gender Code - Subscriber Gender	R	DMG03		Patient-Sex
NM101	2010 BB	Entity Identifier Code - PR	R	NM101	2010B B	Entity Identifier Code - PR
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name - ADHS/BHS	R	NM103		Payor-Name
NM108		Identification Code Qualifier - PI	R	NM108		Identification Code Qualifier - PI
NM109		Identification Code - 86-6004791	R	NM109		Payor-ID
CLM01	2300	Claim Submitters Id - ICN Number	R	CLM01	2300	Memory Variable: CLM01_40-Patient_CTL_NBR

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
CLM02		Monetary Amount - Line Item Charge Amt	R	CLM02		Memory Variable: Total Accom+Total Ancilliary
CLM05		HealthCare Serv. Loc. Info	R	CLM05		
CLM05-1		Facility Code Value - Bill type position 1 and 2	R	CLM05-1		Memory Variable: Facility Type Code
CLM05-2		Facility Code Qualifier - A	R	CLM05-2		Constant A
CLM05-3		Claim Frequency Type Code - Bill type position 3	R	CLM05-3		Memory Variable: Claim Frequency Code
CLM06		Provider Signature on File (Y/N)	R	CLM06		Constant Y
CLM07		Prov. Accept Assign. Code - A	R	CLM07		
CLM08		Yes/No Condition Resp. Code - (Y/N)	R	CLM08		Constant Y
CLM09		Release of Information Code (A, I, M, N, O, Y)	R	CLM09		Constant A
CLM18		Yes/No Condition Resp. Code - N	R	CLM18		Patient. Sign. Source Code - N
CLM20		Delay Reason Code				
DTP01	2300	Date/Time Qualifier - 096	R	DTP01	2300	Currently not mapped, New constant - 096
DTP02		Date Time Period Format Qualifier - TM	R	DTP02		Currently not mapped, New constant - TM
DTP03		Date Time Period - Format: HHMM	R	DTP03		Currently Not Mapped, New field - Discharge-Hour
DTP01	2300	Date/Time Qualifier - 434	R	DTP01	2300	Constant 434
DTP02		Date Time Period Format Qualifier - RD8	R	DTP02		Constant RD8
DTP03		Date Time Period - Format: CCYYMMDD-CCYYMMDD	R	DTP03		Memory Variable: Statement Date
DTP01	2300	Date/Time Qualifier - 435	R	DTP01	2300	Constant 435
DTP02		Date Time Period Format Qualifier - DT	R	DTP02		Constant DT
DTP03		Date Time Period - Format: CCYYMMDDHHMM	R	DTP03		Memory Variable: Admission Date
CL101	2300	Admission type code - 3	S	CL101	2300	Constant 3
CL102		Admission Source Code - Source	S	CL102		Not mapped, New field Admission-Source
CL103		Patient Status Code	S	CL103		Patient-Status
CN101	2300	Contract Type Code - 05 or 02	R	CN101	2300	Currently not mapped, New constant, either 05 or 02
CN102		Monetary Amount - Special Net Value or Net Paid	S	CN102		Currently not mapped, New Field - Special-Net-Value

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
CN103		Percent		CN103		
CN104		Reference Identification		CN104		
CN105		Terms Discount Percent		CN105		
CN106		Version Identifier		CN106		
REF01	2300	Reference Identification Qualifier - F8	R	REF01	2300	Currently not mapped, New constant - F8
REF02		Reference Identification - Claim Original Reference Number	R	REF02		Currently not mapped, New field - Claim-Org-Ref-Num
REF01	2300	Reference Identification Qualifier - G1	R	REF01	2300	Currently not mapped, New constant - G1
REF02		Reference Identification - Prior Auth. Number	R	REF02		Currently not mapped, New field - Prior-Auth-Num
REF01	2300	Reference Identification Qualifier - EA				
REF02		Reference Identification - Medical Record Number				
NTE01	2300	Note Reference Code - ADD	R	NTE01	2300	Currently not mapped - New constant - ADD
NTE02		Description	R	NTE02		Currently not mapped - New field, Note-Desc
HI01	2300	HealthCare Code Info.	R	HI01	2300	
HI01-1		Code List Qualifier Code - BK	R	HI01-1		Code List Qualifier Code - BK
HI01-2		Industry Code - Diagnosis Code	R	HI01-2		Prin-Diag-Code
HI02		HealthCare Code Info.	S	HI02		
HI02-1		Code List Qualifier Code - BJ	R	HI02-1		Conditional Store: HI0201: Condititional Store Variable
HI02-2		Industry Code - Admitting Diagnosis Code	R	HI02-2		Admitting-Diag-Code
HI03		HealthCare Code Info.	S	HI03		HealthCare Code Info.
HI03-1		Code List Qualifier Code - BN	R	HI03-1		Currently not mapped - New constant - BN
HI03-2		Industry Code - Trauma Code	R	HI03-2		Curently not mapped - New field, Conditional Store: HI0301
HI01	2300	HealthCare Code Info.	R	HI01	2300	
HI01-1		Code List Qualifier Code - BF	R	HI01-1		Code List Qualifier Code - BF
HI01-2		Industry Code - Diagnosis Code	R	HI01-2		Other-Diag1
HI02		HealthCare Code Info.	S	HI02		
HI02-1		Code List Qualifier Code - BF	R	HI02-1		Constant BF
HI02-2		Industry Code - Diagnosis Code	R	HI02-2		Other-Diag2

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
HI03		HealthCare Code Info.	S	HI03		
HI03-1		Code List Qualifier Code - BF	R	HI03-1		Constant BF
HI03-2		Industry Code - Diagnosis Code	R	HI03-2		Other-Diag3
HI04		HealthCare Code Info.	S	HI04		
HI04-1		Code List Qualifier Code - BF	R	HI04-1		Constant BF
HI04-2		Industry Code - Diagnosis Code	R	HI04-2		Other-Diag4
HI05		HealthCare Code Info.	S	HI05		
HI05-1		Code List Qualifier Code - BF	R	HI05-1		Constant BF
HI05-2		Industry Code - Diagnosis Code	R	HI05-2		Other-Diag5
HI06		HealthCare Code Info.	S	HI06		
HI06-1		Code List Qualifier Code - BF	R	HI06-1		Constant BF
HI06-2		Industry Code - Diagnosis Code	R	HI06-2		Other-Diag6
HI07		HealthCare Code Info.	S	HI07		
HI07-1		Code List Qualifier Code - BF	R	HI07-1		Constant BF
HI07-2		Industry Code - Diagnosis Code	R	HI07-2		Other-Diag7
HI08		HealthCare Code Info.	S	HI08		
HI08-1		Code List Qualifier Code - BF	R	HI08-1		Constant BF
HI08-2		Industry Code - Diagnosis Code	R	HI08-2		Other-Diag8
HI09		HealthCare Code Info.	S	HI09		
HI09-1		Industry Code - Diagnosis Code	R	HI09-1		
HI09-2		HealthCare Code Info.	S	HI09-2		
HI010		Code List Qualifier Code - BF	R	HI010		
HI010-1		Industry Code - Diagnosis Code Code	R	HI010-1		
HI010-2		HealthCare Code Info.	S	HI010-2		
HI011		Code List Qualifier Code - BF	R	HI011		
HI011-1		Industry Code - Diagnosis Code	R	HI011-1		
HI011-2		HealthCare Code Info.	S	HI011-2		
HI012		Code List Qualifier Code - BF	R	HI012		

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
HI012-1		Industry Code - Diagnosis Code	R	HI012-1		
HI012-2		HealthCare Code Info.	S	HI012-2		
HI01	2300	HealthCare Code Info.	R	HI01	2300	
HI01-1		Code List Qualifier Code - BR	R	HI01-1		Code List Qualifier Code - BR
HI01-2		Industry Code - ICD9 Procedures Code	R	HI01-2		Prin-Proc-Code
HI01-3		Date Time Period Format Qualifier - D8	S	HI01-3		Constant D8
HI01-4		Date Time Period - ICD9 Procedure Date	S	HI01-4		Prin-Proc-Date
HI01	2300	HealthCare Code Info.	R	HI01	2300	
HI01-1		Code List Qualifier Code - BR	R	HI01-1		Code List Qualifier Code - BR
HI01-2		Industry Code - ICD9 Procedures Code	R	HI01-2		Other-Proc-Code2
HI01-3		Date Time Period Format Qualifier - D8	R	HI01-3		Constant D8
HI01-4		Date Time Period - ICD9 Procedure Date	R	HI01-4		Other-Proc-Date2
HI02		HealthCare Code Info.	S	HI02		
HI02-1		Code List Qualifier Code - BQ	R	HI02-1		Code List Qualifier Code - BQ
HI02-2		Industry Code - ICD9 Procedures Code	R	HI02-2		Other-Proc-Code3
HI02-3		Date Time Period Format Qualifier - D8	S	HI02-3		Constant D8
HI02-4		Date Time Period - ICD9 Procedure Date	S	HI02-4		Other-Proc-Date3
HI03		HealthCare Code Info.	S	HI03		
HI03-1		Code List Qualifier Code - BQ	R	HI03-1		Code List Qualifier Code - BQ
HI03-2		Industry Code - ICD9 Procedures Code	R	HI03-2		Other-Proc-Code-4
HI03-3		Date Time Period Format Qualifier - D8	S	HI03-3		Constant D8
HI03-4		Date Time Period - ICD9 Procedure Date	S	HI03-4		Other-Proc-Date4
HI04		HealthCare Code Info.	S	HI04		
HI04-1		Code List Qualifier Code - BQ	R	HI04-1		Code List Qualifier Code - BQ
HI04-2		Industry Code - ICD9 Procedures Code	R	HI04-2		Other-Proc-Code5
HI04-3		Date Time Period Format Qualifier - D8	S	HI04-3		Constant D8
HI04-4		Date Time Period - ICD9 Procedure Date	S	HI04-4		Other-Proc-Date5

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
HI05				HI05		
HI05-1		Code List Qualifier Code - BQ	R	HI05-1		
HI05-2		Industry Code - ICD9 Procedures Code	R	HI05-2		
HI05-3		Date Time Period Format Qualifier - D8	S	HI05-3		
HI05-4		Date Time Period - ICD9 Procedure Date	S	HI05-4		
HI06				HI06		
HI06-1		Code List Qualifier Code - BQ	R	HI06-1		
HI06-2		Industry Code - ICD9 Procedures Code	R	HI06-2		
HI06-3		Date Time Period Format Qualifier - D8	S	HI06-3		
HI06-4		Date Time Period - ICD9 Procedure Date	S	HI06-4		
HI07				HI07		
HI07-1		Code List Qualifier Code - BQ	R	HI07-1		
HI07-2		Industry Code - ICD9 Procedures Code	R	HI07-2		
HI07-3		Date Time Period Format Qualifier - D8	S	HI07-3		
HI07-4		Date Time Period - ICD9 Procedure Date	S	HI07-4		
HI08				HI08		
HI08-1		Code List Qualifier Code - BQ	R	HI08-1		
HI08-2		Industry Code - ICD9 Procedures Code	R	HI08-2		
HI08-3		Date Time Period Format Qualifier - D8	S	HI08-3		
HI08-4		Date Time Period - ICD9 Procedure Date	S	HI08-4		
HI09				HI09		
HI09-1		Code List Qualifier Code - BQ	R	HI09-1		
HI09-2		Industry Code - ICD9 Procedures Code	R	HI09-2		
HI09-3		Date Time Period Format Qualifier - D8	S	HI09-3		
HI09-4		Date Time Period - ICD9 Procedure Date	S	HI09-4		
HI010				HI010		
HI010-1		Code List Qualifier Code - BQ	R	HI010-1		

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
HI010-2		Industry Code - ICD9 Procedures Code	R	HI010-2		
HI010-3		Date Time Period Format Qualifier - D8	S	HI010-3		
HI010-4		Date Time Period - ICD9 Procedure Date	S	HI010-4		
HI011				HI011		
HI011-1		Code List Qualifier Code - BQ	R	HI011-1		
HI011-2		Industry Code - ICD9 Procedures Code	R	HI011-2		
HI011-3		Date Time Period Format Qualifier - D8	S	HI011-3		
HI011-4		Date Time Period - ICD9 Procedure Date	S	HI011-4		
HI012				HI012		
HI012-1		Code List Qualifier Code - BQ	R	HI012-1		
HI012-2		Industry Code - ICD9 Procedures Code	R	HI012-2		
HI012-3		Date Time Period Format Qualifier - D8	S	HI012-3		
HI012-4		Date Time Period - ICD9 Procedure Date	S	HI012-4		
HI01	2300	HealthCare Code Info.	R	HI01	2300	HealthCare Code Info.
HI01-1		Code List Qualifier Code - BH	R	HI01-1		Code List Qualifier Code - BH
HI01-2		Industry Code - Occurrence Code	R	HI01-2		Occ-Code-1
HI01-3		Date Time Period Format Qualifier - D8	S	HI01-3		Date Time Period Format Qualifier - D8
HI01-4		Date Time Period - ICD9 Occurrence Date	S	HI01-4		Occ-Date-1
HI02		HealthCare Code Info.	R	HI02		HealthCare Code Info.
HI02-1		Code List Qualifier Code - BH	R	HI02-1		Code List Qualifier Code - BH
HI02-2		Industry Code - Occurrence Code	R	HI02-2		Occ-Code-2
HI02-3		Date Time Period Format Qualifier - D8	S	HI02-3		Date Time Period Format Qualifier - D8
HI02-4		Date Time Period - Occurrence Date	S	HI02-4		Occ-Date-2
HI03		HealthCare Code Info.	R	HI03		
HI03-1		Code List Qualifier Code - BH	R	HI03-1		Code List Qualifier Code - BH
HI03-2		Industry Code - Occurrence Code	R	HI03-2		Occ-Code-3
HI03-3		Date Time Period Format Qualifier - D8	S	HI03-3		Date Time Period Format Qualifier - D8

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
HI03-4		Date Time Period - Occurrence Date	S	HI03-4		Occ-Date-3
HI04		HealthCare Code Info.		HI04		
HI04-1		Code List Qualifier Code - BH	R	HI04-1		Code List Qualifier Code - BH
HI04-2		Industry Code - Occurrence Code	R	HI04-2		Occ-Code-4
HI04-3		Date Time Period Format Qualifier - D8	S	HI04-3		Date Time Period Format Qualifier - D8
HI04-4		Date Time Period - Occurrence Date	S	HI04-4		Occ-Date-4
HI05		HealthCare Code Info.		HI05		
HI05-1		Code List Qualifier Code - BH	R	HI05-1		Code List Qualifier Code - BH
HI05-2		Industry Code - Occurenence Code	R	HI05-2		Occ-Code-5
HI05-3		Date Time Period Format Qualifier - D8	S	HI05-3		Date Time Period Format Qualifier - D8
HI05-4		Date Time Period - Occurrence Date	S	HI05-4		Occ-Date-5
HI06		HealthCare Code Info.		HI06		
HI06-1		Code List Qualifier Code - BH	R	HI06-1		Code List Qualifier Code - BH
HI06-2		Industry Code - Occurrence Code	R	HI06-2		Occ-Code-6
HI06-3		Date Time Period Format Qualifier - D8	S	HI06-3		Date Time Period Format Qualifier - D8
HI06-4		Date Time Period - Occurrence Date	S	HI06-4		Occ-Date-6
HI07		HealthCare Code Info.		HI07		
HI07-1		Code List Qualifier Code - BH	R	HI07-1		Code List Qualifier Code - BH
HI07-2		Industry Code - Occurrence Code	R	HI07-2		Occ-Code-7
HI07-3		Date Time Period Format Qualifier - D8	S	HI07-3		Date Time Period Format Qualifier - D8
HI07-4		Date Time Period - Occurrence Date	S	HI07-4		Occ-Date-7
HI08		HealthCare Code Info.		HI08		
HI08-1		Code List Qualifier Code - BH	R	HI08-1		Code List Qualifier Code - BH
HI08-2		Industry Code - Occurrence Code	R	HI08-2		Occ-Code-8
HI08-3		Date Time Period Format Qualifier - D8	S	HI08-3		Date Time Period Format Qualifier - D8
HI08-4		Date Time Period - Occurrence Date	S	HI08-4		Occ-Date-8
HI09		HealthCare Code Info.	S	HI09		

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
HI09-1		Code List Qualifier Code - BH	R	HI09-1		
HI09-2		Industry Code - Occurrence Code	R	HI09-2		
HI09-3		Date Time Period Format Qualifier - D8	S	HI09-3		
HI09-4		Date Time Period - Occurrence Date	S	HI09-4		
HI010				HI010		
HI010-1		Code List Qualifier Code - BH	R	HI010-1		
HI010-2		Industry Code - Occurrence Code	R	HI010-2		
HI010-3		Date Time Period Format Qualifier - D8	S	HI010-3		
HI010-4		Date Time Period - Occurrence Date	S	HI010-4		
HI011				HI011		
HI011-1		Code List Qualifier Code - BH	R	HI011-1		
HI011-2		Industry Code - Occurrence Code	R	HI011-2		
HI011-3		Date Time Period Format Qualifier - D8	S	HI011-3		
HI011-4		Date Time Period - Occurrence Date	S	HI011-4		
HI012				HI012		
HI012-1		Code List Qualifier Code - BH	R	HI012-1		
HI012-2		Industry Code - Occurrence Code	R	HI012-2		
HI012-3		Date Time Period Format Qualifier - D8	S	HI012-3		
HI012-4		Date Time Period - Occurrence Date	S	HI012-4		
HI01	2300	HealthCare Code Info.	R	HI01	2300	HealthCare Code Info.
HI01-1		Code List Qualifier Code - BE	R	HI01-1		Code List Qualifier Code - BE
HI01-2		Industry Code - Value Code - A2	R	HI01-2		Value-Code-1
HI01-5		Monetary Amount	R	HI01-5		Value-Amount-1
HI02		HealthCare Code Info.	R	HI02		
HI02-1		Code List Qualifier Code - BE	R	HI02-1		
HI02-2		Industry Code - Value Code - A2	R	HI02-2		
HI02-5		Monetary Amount	R	HI02-5		
HI03		HealthCare Code Info.	R	HI03		

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
HI03-1		Code List Qualifier Code - BE	R	HI03-1		
HI03-2		Industry Code - Value Code - A2	R	HI03-2		
HI03-5		Monetary Amount	R	HI03-5		
HI04	2300	HealthCare Code Info.	R	HI04	2300	
HI04-1		Code List Qualifier Code - BE	R	HI04-1		
HI04-2		Industry Code - Value Code - A2	R	HI04-2		
HI04-5		Monetary Amount	R	HI04-5		
HI05		HealthCare Code Info.	R	HI05		
HI05-1		Code List Qualifier Code - BE	R	HI05-1		
HI05-2		Industry Code - Value Code - A2	R	HI05-2		
HI05-5		Monetary Amount	R	HI05-5		
HI06		HealthCare Code Info.	R	HI06		
HI06-1		Code List Qualifier Code - BE	R	HI06-1		
HI06-2		Industry Code - Value Code - A2	R	HI06-2		
HI06-5		Monetary Amount	R	HI06-5		
HI07		HealthCare Code Info.	R	HI07		
HI07-1		Code List Qualifier Code - BE	R	HI07-1		
HI07-2		Industry Code - Value Code - A2	R	HI07-2		
HI07-5		Monetary Amount	R	HI07-5		
HI08		HealthCare Code Info.	R	HI08		
HI08-1		Code List Qualifier Code - BE	R	HI08-1		
HI08-2		Industry Code - Value Code - A2	R	HI08-2		
HI08-5		Monetary Amount	R	HI08-5		
HI09		HealthCare Code Info.	R	HI09		
HI09-1		Code List Qualifier Code - BE	R	HI09-1		
HI09-2		Industry Code - Value Code - A2	R	HI09-2		
HI09-5		Monetary Amount	R	HI09-5		
HI010		HealthCare Code Info.	R	HI010		
HI010-1		Code List Qualifier Code - BE	R	HI010-1		

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
HI010-2		Industry Code - Value Code - A2	R	HI010-2		
HI010-5		Monetary Amount	R	HI010-5		
HI011		HealthCare Code Info.	R	HI011		
HI011-1		Code List Qualifier Code - BE	R	HI011-1		
HI011-2		Industry Code - Value Code - A2	R	HI011-2		
HI011-5		Monetary Amount	R	HI011-5		
HI012		HealthCare Code Info.	R	HI012		
HI012-1		Code List Qualifier Code - BE	R	HI012-1		
HI012-2		Industry Code - Value Code - A2	R	HI012-2		
HI012-5		Monetary Amount	R	HI012-5		
NM101	2310 A	Entity Identifier Code - 71	R	NM101	2310A	Constant - 71
NM102		Entity Type Qualifier - 1	R	NM102		Constant - 1
NM103		Name Last / Org. Name	R	NM103		Memory Variable: Attending Physician Last Name
NM104		Name First	S	NM104		
NM105		Name Middle	S	NM105		
NM107		Name Suffix	S	NM107		
NM108		Identification Code Qualifier - 24	R	NM108		Constant - 24
NM109		Identification Code - Attending Physicians EIN	R	NM109		Attending-PHY-EIN
SBR01	2320	Payer Resp. Seq. Num Code - (P/S/T)	R	SBR01	2320	Currently not mapped, New field - Payor-Resp
SBR02		Individual Relationship Code - 18	R	SBR02		Currently not mapped, New constant - 18
SBR03		Reference Identifier		SBR03		
SBR04		Name		SBR04		
SBR09		Claim Filing Indicator Code - CI	S	SBR09		Currently not mapped - New constant - CI
AMT01	2320	Amount Qualifier Code - C4	R	AMT01	2320	Currently not mapped - New constant - C4
AMT02		Monetary Amount - Other Insurance Payment	R	AMT02		Currently not mapped - New field, Medicare-Allowed
DMG01	2320	Date Time Period Form.Qual. - D8	R	DMG01	2320	Currently not mapped - New constant - D8
DMG02		Date Time Period - Subscriber DOB	R	DMG02		Currently not mapped - New field, Other-Sub-DOB
DMG03		Gender Code - Subscriber Gender	R	DMG03		Currently not mapped - New field, Other-Sub-Gender

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
NM101	2330A	Entity Identifier Code - IL	R	NM101	2330A	Currently not mapped - New constant - IL
NM102		Entity Type Qualifier - 1	R	NM102		Currently not mapped - New constant - 1
NM103		Name Last / Org. Name - Client's Last Name	R	NM103		Currently not mapped - New Field Other Subscriber-Name
NM104		Name First	S	NM104		
NM105		Name Middle	S	NM105		
NM107		Name Suffix	S	NM107		
NM108		Identification Code Qualifier - MI	R	NM108		Currently not mapped - New constant - MI
NM109		Identification Code - Client's other ins. ID	R	NM109		Currently not mapped - New field, Other-Ins-ID
NM101	2330B	Entity Identifier Code - PR	R	NM101	2330B	Currently not mapped, New constant - PR
NM102		Entity Type Qualifier - 2	R	NM102		Currently not mapped, New constant - 2
NM103		Name Last / Org. Name - Other ins. Company Name	R	NM103		Currently not mapped, New field - Other-Ins-Company-Name
NM108		Identification Code Qualifier - PI	R	NM108		Currently not mapped, New constant - PI
NM109		Identification Code - 003	R	NM109		Currently not mapped, New constant - 003
SBR01	2320	Payer Resp. Seq. Num Code (P/S/T)	R	SBR01	2320	Currently not mapped, New field - Payor-Resp-2
SBR02		Individual Relationship Code - 18	R	SBR02		Currently not mapped, New constant - 18
SBR03		Reference Identifier		SBR03		
SBR04		Name		SBR04		
SBR09		Claim Filing Indicator Code - MA or MB	S	SBR09		Currently not mapped, New constant - Either MA or MB (Business Decision.)
CAS01	2320	Claim Adjustment Group Code - PR	S	CAS01	2320	Currently not mapped, new constant - PR
CAS02		Claim Adjustment Reason Code - 1	R	CAS02		Currently not mapped, new constant - 1
CAS03		Monetary Amount - Medicare Deductible	R	CAS03		Currently not mapped, new field - Medicare-Deductible
CAS04		Quantity	R	CAS04		Currently not mapped, new field - Quantity
CAS05		Claim Adjustment Reason Code	S			
CAS06		Monetary Amount	S			
CAS07		Quantity	S			
CAS08		Claim Adjustment Reason Code	S			

ADHS/DBHS				GREABHA		
Segment ID	Loop	Element Name	Usage	Segment ID	Loop	Element Name
CAS09		Monetary Amount	S			
CAS10		Quantity	S			
CAS11		Claim Adjustment Reason Code	S			
CAS12		Monetary Amount	S			
CAS13		Quantity	S			
CAS14		Claim Adjustment Reason Code	S			
CAS15		Monetary Amount	S			
CAS16		Quantity	S			
CAS17		Claim Adjustment Reason Code	S			
CAS18		Monetary Amount	S			
CAS19		Quantity	S			
AMT01	2320	Amount Qualifier Code - B6	R	AMT01	2320	Not currently mapped - New constant - B6
AMT02		Monetary Amount - Medicare Allow Amount	R	AMT02		Not currently mapped, New field - Medicare-Allow-Amount
AMT01	2320	Amount Qualifier Code - N1	R	AMT01	2320	Not currently mapped, New constant - N1
AMT02		Monetary Amount - Medicare Payment	R	AMT02		Not currently mapped, New field Other-Insurance-Payment
OI03	2320	Yes/No Condition Resp. Code - Y/N	R	OI03	2320	Not currently mapped - New constant - Y
OI06		Release of Information Code - A, I, M, N, O, or Y	R	OI06		Not currently mapped - New constant - A
NM101	2330 A	Entity Identifier Code - IL	R	NM101	2330A	Not currently mapped - New constant - IL
NM102		Entity Type Qualifier - 1	R	NM102		Not currently mapped - New constant - 1
NM103		Name Last / Org. Name - Client's Last Name	R	NM103		Not currently mapped, New field - Ins-Last-Name-2
NM104		Name First	S	NM104		Not currently mapped, New field - Ins-First-Name-2
NM105		Name Middle	S	NM105		
NM107		Name Suffix	S	NM107		
NM108		Identification Code Qualifier - MI	R	NM108		Not currently mapped, New constant - MI
NM109		Identification Code - Client's Medicare ID	R	NM109		Not currently mapped, New field - Insureds-ID-Num-2
NM101	2330 B	Entity Identifier Code - PR	R	NM101	2330B	Not currently mapped, New content - PR

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
NM102		Entity Type Qualifier - 2	R	NM102		Not currently mapped, New constant - 2
NM103		Name Last / Org. Name - Medicare	R	NM103		Not currently mapped, New field - Payor-Name-2
NM108		Identification Code Qualifier - PI	R	NM108		Not currently mapped, New constant - PI
NM109		Identification Code - 002	R	NM109		Not currently mapped, New field - Payor-Org-ID-2
LX01	2400	Assigned Number	R	LX01	2400	Memory Variable: LX01 : Assigned Number Counter
SV201		Product Service/ID - Service Line Rev. Code	R	SV201		Revenue-Code
SV202		Composite Medical Procedure Identifier	S	SV202		
SV202-1		Produce Service ID Qualifier - HC or N4	R	SV202-1		Memory Variable: SV20201
SV202-2		Procedure Code	R	SV202-2		HCPCS-Proc-Code
SV202-3		Procedure Modifier	S	SV202-3		
SV202-4		Procedure Modifier	S	SV202-4		
SV202-5		Procedure Modifier	S	SV202-5		
SV202-6		Procedure Modifier	S	SV202-6		
SV203		Line Item Charge Amount	R	SV203		Total-Charges-2
SV204		Unit or Basis for Measurement Code - Codes: DA, F2, or UN	R	SV204		Constant - UN
SV205		Quantity	R	SV205		Units-Of-Service
SV206		Unit Rate	S	SV206		Currently not mapped, New field - Unit-Rate
SV207		Monetary Amount - Line Item Non Covered Charge Amt	S	SV207		Noncovered-Charges
SE01		Number of Included Segments - Total Number of segments	R	SE01		Number of Included Segments - Total Number of segments
SE02		Trans. Set Control Number	R	SE02		

1

***Data Map* - 837 Professional file**

Following is the data map for the 837 Professional file, specific to ADHS/DBHS:

ADHS/DBHS				GREABHA		
Segment ID	**Loop**	**Element Name**	**Usage**	**Segment ID**	**Loop**	**Element Name**
ST01		Trans. Set Header - 837	R	ST01		Trans. Set Header - 837
ST02		Trans. Set Control Number - Incremented Number	R	ST02		Trans. Set Control Number - Incremented Number
BHT01		Hierarchical Structure Code - 0019	R	BHT01		Hierarchical Structure Code - 0019
BHT02		Trans. Set Purpose Code - 00	R	BHT02		Trans. Set Purpose Code - 00
BHT03		Reference Identifier	R	BHT03		Submission-NBR
BHT04		Date	R	BHT04		Create-Date
BHT05		Time	R	BHT05		Submit-Time
BHT06		Trans. Type Code - RP	R	BHT06		Transaction Type Code RP
REF01		Reference I.D. Qualifier - 87	R	REF01		Reference Identification Qualifier - 87
REF02		Reference Identifier - 00410X098A1	R	REF02		Reference Identifier - 00401X098A1
NM101	1000A	Entity Identifier Code - 41	R	NM101	1000A	Entity Identifier Code - 41
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name - RBHA Name	R	NM103		Receiver
NM104		Name First		NM104		
NM105		Name Middle		NM105		
NM108		Identification Code Qualifier - 46	R	NM108		Identification Code Qualifier - 46
NM109		Identification Code - RBHA ID	R	NM109		Identification Code - 401M
PER01	1000A	Contact Function Code - IC	R	PER01	1000A	Contact Function Code - IC
PER02		Name	R	PER02		Name - Centene
PER03		Comm. Number Qualifier	R	PER03		Comm. Number Qualifier
PER04		Comm. Number	R	PER04		Submitter-Phone
PER05		Comm. Number Qualifier		PER05		
PER06		Comm Number		PER06		
PER07		Comm. Number Qualifier		PER07		
PER08		Comm. Number		PER08		
NM101	1000B	Entity Identifier Code -	R	NM101	1000B	Entity Identifier Code -

ADHS/DBHS				GREABHA		
		40				40
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name	R	NM103		Receiver
NM108		Identification Code Qualifier - 46	R	NM108		Identification Code Qualifier - 46
NM109		Identification Code	R	NM109		Receiver-ID
HL01	2000A	Hierarchical ID Number	R	HL01	2000A	Memory Variable HL01 Hierarchical Level Counter
HL03		Hierarchical Level Code - 20	R	HL03		Hierarchical Level Code - 20
HL04		Hierarchical Child Code - 1	R	HL04		Hierarchical Child Code - 1
NM101	2010AA	Entity Identifier Code - 85	R	NM101	2010AA	Entity Identifier Code - 85
NM102		Entity Type Qualifier - 1	R	NM102		Entity Type Qualifier -1
NM103		Name Last / Org. Name	R	NM103		Prov-Last-Name/Prov-Org-Name
NM108		Identification Code Qualifier - 24	R	NM108		Identification Code Qualifier - 24
NM109		Identification Code	R	NM109		Prov-Mcd-Num
N301	2010AA	Address Information	R	N301	2010AA	Prov-Serv-Addr
N302		Address Information		N302		
N401		City Name	R	N401		Prov-Serv-City
N402		State or Providence Code	R	N402		Prov-Serv-State
N403		Postal Code	R	N403		Prov-Serv-Zipcode
N404		Country Code		N404		
REF01	2010AA	Reference Ident. Qualifier - 1D	R	REF01	2010AA	Reference Ident. Qualifier - 1D
REF02		Reference Identifier	R	REF02		Prov-Medicaid-NBR
NM101	2010AB	Entity Identifier Code - 87	R	NM101	2010AB	Currently Not Mapped, New constant - 87
NM102		Entity Type Qualifier - 2	R	NM102		Currently Not Mapped, New constant - 2
NM103		Name Last / Org. Name	R	NM103		Currently Not Mapped, New field - Pay-To-Provider-Name
NM108		Identification Code Qualifier - 24	R	NM108		Currently Not Mapped, New constant - 24
NM109		Identification Code	R	NM109		Currently Not Mapped, New field, PayToProvider-EIN
N301	2010AB	Address Information	R	N301	2010AB	Currently Not Mapped, New field, PayToProvider-Address1
N302		Address Information		N302		

ADHS/DBHS					GREABHA		
N401	2010AB	City Name	R		N401	2010AB	Currently Not Mapped, New field, PayToProvider-City
N402		State or Providence Code	R		N402		Currently Not Mapped, New field, PayToProvider-State
N403		Postal Code	R		N403		Currently Not Mapped, New field, PayToProvider-Zipcode
N404		Country Code			N404		
REF01	2010AB	Reference Ident. Qualifier - G2	R		REF01	2010AB	Curently Not Mapped, New constant- G2
REF02		Reference Identifier - Provider ID	R		REF02		Curently Not Mapped, New field - PayToProvider- ID
HL01	2000B	Hierarchical ID Number	R		HL01	2000B	Memory Variable: HL01: Hierarchical Level Counter
HL02		Hierarchical Parent ID Num - 1	R		HL02		Hierarchical Parent ID Num - 1
HL03		Hierarchical Level Code - 22	R		HL03		Hierarchical Level Code - 22
HL04		Hierarchical Child Code - 0	R		HL04		Hierarchical Child Code - 0
SBR01	2000B	Payer Resp. Seq. Num Code - T	R		SBR01	2000B	Payer Resp. Seq. Num Code - T
SBR02		Individual Relationship Code - 18	S		SBR02		Individual Relationship Code - 18
SBR03		Reference Identifier			SBR03		
SBR04		Name			SBR04		
SBR05		Insurance Type Code			SBR05		
SBR09		Claim Filing Indicator Code - MC	S		SBR09		Claim Filing Indicator Code - MC
NM101	2010BA	Entity Identifier Code - IL	R		NM101	2010BA	Entity Identifier Code - IL
NM102		Entity Type Qualifier - 1	R		NM102		Entity Type Qualifier - 1
NM103		Name Last / Org. Name	R		NM103		Pat-Last-Name
NM104		Name First	R		NM104		Pat-First-Name
NM105		Name Middle			NM105		
NM107		Name Suffix			NM107		
NM108		Identification Code Qualifier - MI	R		NM108		Identification Code Qualifier - MI
NM109		Identification Code	R		NM109		Insured-Id-Num
N301	2010BA	Address Information	R		N301	2010BA	Pat-Addr1
N302		Address Information			N302		
N401	2010BA	City Name	R		N401	2010BA	Pat-City
N402		State or Providence Code	R		N402		Pat-State

ADHS/DBHS					GREABHA		
N403		Postal Code	R		N403		Pat-Zip
N404		Country Code			N404		
DMG01	2010BA	Date Time Period Form.Qual. - D8	R		DMG01	2010BA	Date Time Period Form.Qual. - D8
DMG02		Date Time Period	R		DMG02		Pat-DOB
DMG03		Gender Code	R		DMG03		Pat-Sex
NM101	2010BB	Entity Identifier Code - PR	R		NM101	2010BB	Entity Identifier Code - PR
NM102		Entity Type Qualifier - 2	R		NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name - ADHS/BHS	R		NM103		Payor-Name
NM108		Identification Code Qualifier - PI	R		NM108		Identification Code Qualifier - PI
NM109		Identification Code - 866004791	R		NM109		Payor-Org-ID
CLM01	2300	Claim Submitters Id - ICN Number	R		CLM01	2300	Memory Variable: CLM01_CA0:3 CLM01_CA0:3
CLM02		Monetary Amount - Line Item Charge Amt	R		CLM02		Total-Amount
CLM05		HealthCare Serv. Loc. Info	R		CLM05		HealthCare Serv. Loc. Info
CLM05-1		Facility Code Value - POS	R		CLM05-1		Place-Of-Service
CLM05-3		Claim Frequency Type Code - 1	R		CLM05-3		Claim Frequency Type Code - 1
CLM06		Yes/No Condition Resp. Code - Y	R		CLM06		Prov-Sign-On-File
CLM07		Prov. Accept Assign. Code - A	R		CLM07		Prov-Assign-Ind
CLM08		Yes/No Condition Resp. Code - Y	R		CLM08		Assign-Benefit-Ind
CLM09		Release of Information Code (A, I, M, O, Y)	R		CLM09		Release-Info-Ind
CLM10		Patient. Sign. Source Code	S		CLM10		Patient. Sign. Source Code - C
CLM11		Related Causes Info.			CLM11		
CLM11-1		Related Causes Code			CLM11-1		
CLM11-2		Related Causes Code			CLM11-2		
CLM11-3		Related Causes Code			CLM11-3		
CLM11-4		State or Providence Code			CLM11-4		
CLM11-5		Country Code			CLM11-5		
CLM12		Special Program Code			CLM12		
CLM16		Provider Agreement Code			CLM16		
CLM20		Delay Reason Code			CLM20		
REF01	2300	Reference Ident.	R		REF01	2300	Currently not mapped -

ADHS/DBHS				GREABHA		
		Qualifier - G1				New constant - G1
REF02		Reference Identifier - Prior Auth Number	R	REF02		Currently not mapped - New field, Prior-Auth
REF01	2300	Reference Ident. Qualifier		REF01		
REF02		Reference Identifier		REF02		
NTE01	2300	Note Reference Code - ADD	R	NTE01	2300	Currently not mapped - New constant - ADD
NTE02		Description	R	NTE02		Currently not mapped - New field, Note-Desc
HI01	2300	HealthCare Code Info.	R	HI01	2300	
HI01-1		Code List Qualifier Code - BK	R	HI01-1		Code List Qualifier Code - BK
HI01-2		Industry Code - Diagnosis Code	R	HI01-2		Diagnosis-Cd1
HI02		HealthCare Code Info.	S	HI02		
HI02-1		Code List Qualifier Code - BF	R	HI02-1		Conditional Store: HI0201: Condititional Store Variable
HI02-2		Industry Code - ICD9 Code 2	R	HI02-2		Diagnosis-Cd2
HI03		HealthCare Code Info.	S	HI03		HealthCare Code Info.
HI03-1		Code List Qualifier Code - BF	R	HI03-1		Currently not mapped - New constant - BF
HI03-2		Industry Code - ICD9 Code 3	R	HI03-2		Curently not mapped - New field, Conditional Store: HI0301
HI04		HealthCare Code Info.	S	HI04		HealthCare Code Info.
HI04-1		Code List Qualifier Code - BF	R	HI04-1		Currently not mapped - New constant - BF
HI04-2		Industry Code - ICD9 Code 4	R	HI04-2		Currently not mapped - New field, Conditional Store: HI0401
NM101	2310B	Entity Identifier Code	R	NM101	2310B	Currently not mapped - New constant - 82
NM102		Entity Type Qualifier	R	NM102		Currently not mapped - New constant - 2
NM103		Name Last / Org. Name	R	NM103		Currently not mapped - New field, Rendering-Prov
NM108		Identification Code Qualifier	R	NM108		Currently not mapped - New constant - 24
NM109		Identification Code	R	NM109		Currently not mapped - New field, Rendering-ID-CD
SBR01	2320	Payer Resp. Seq. Num Code - (P/S)	R	SBR01	2320	Memory Variable: PayorRespCode: Payor Responsibility Seq. Cd
SBR02		Individual Relationship Code - 18	R	SBR02		Memory Variable: PatientRelationship : Patient Relationship to Insured

ADHS/DBHS				GREABHA		
SBR03		Reference Identifier		SBR03		
SBR04		Name		SBR04		
SBR05		Insurance Type Code - MB or MP	R	SBR05		Not Mapped - New field, Insurance-Type
SBR09		Claim Filing Indicator Code - MB	S	SBR09		Claim Filing Indicator Code - MC
AMT02		Monetary Amount - Medicare Payment	R	AMT02		Currently not mapped - New field, Medicare-Pay
AMT01	2320	Amount Qualifier Code - B6	R	AMT01	2320	Currently not mapped - New constant - B6
AMT02		Monetary Amount	R	AMT02		Currently not mapped - New field, Medicare-Allowed
AMT01	2320	Amount Qualifier Code	R	AMT01	2320	Currently not mapped - New constant - F2
AMT02		Monetary Amount	R	AMT02		Currently not mapped - New field, Medicare-Deductible
DMG01	2320	Date Time Period Form.Qual. - D8	R	DMG01	2320	Date Time Period Form.Qual. - D8
DMG02		Date Time Period	R	DMG02		Ins-Dob
DMG03		Gender Code	R	DMG03		Ins-Sex
OI03	2320	Yes/No Condition Resp. Code - Y	R	OI03	2320	Assign-Benefit-Ind
OI04		Patients Signature Source Cd. - C	S	OI04		Signature-Source
OI06		Release of Information Code - A	R	OI06		Currently not mapped - New field, Rel-Info-Code
NM101	2330A	Entity Identifier Code - IL	R	NM101	2330A	Entity Identifier Code - IL
NM102		Entity Type Qualifier - 1	R	NM102		Entity Type Qualifier - 1
NM103		Name Last / Org. Name	R	NM103		Ins-Last-Name
NM104		Name First	S	NM104		Ins-First-Name
NM105		Name Middle		NM105		
NM107		Name Suffix		NM107		
NM108		Identification Code Qualifier - MI	R	NM108		Identification Code Qualifier - MI
NM109		Identification Code - Client's Medicare IC	R	NM109		Insured-ID-Num
NM101	2330B	Entity Identifier Code - PR	R	NM101	2330B	Entity Identifier Code - PR
NM102		Entity Type Qualifier - 2	R	NM102		Entity Type Qualifier - 2
NM103		Name Last / Org. Name	R	NM103		Payor-Name
NM108		Identification Code Qualifier - PI	R	NM108		Identification Code Qualifier - PI
NM109		Identification Code	R	NM109		Payor-Org-ID

ADHS/DBHS					GREABHA		
SBR01	2320	Payer Resp. Seq. Num Code	R		SBR01	2320	Not currently mapped - New Memory Variable: PayorRespCode: Payor Responsibility Seq. Cd - 2
SBR02		Individual Relationship Code - 18	R		SBR02		Not currently mapped - New constant - 18
SBR03		Reference Identifier			SBR03		
SBR04		Name			SBR04		
SBR05		Insurance Type Code - C1	R		SBR05		Not currently mapped - New Memory Variable: Memory Variable: PatientRelationship : Patient Relationship to Insured - 2
SBR09		Claim Filing Indicator Code	S		SBR09		Not currently mapped, New field Claim-Filing-Ind-2
AMT01	2320	Amount Qualifier Code - D	R		AMT01	2320	Not currently mapped - New constant - D
AMT02		Monetary Amount - Other Insurance Payment	R		AMT02		Not currently mapped, New field Other-Insurance-Payment
DMG01	2320	Date Time Period Form.Qual. - D8	R		DMG01	2320	Not currently mapped - New constant - D8
DMG02		Date Time Period	R		DMG02		Not currently mapped, New field - Subscribers-DOB-2
DMG03		Gender Code	R		DMG03		Not currently mapped, New field- Subscribers-Sex
OI03	2320	Yes/No Condition Resp. Code - Y	R		OI03	2320	Not currently mapped - New constant - Y
OI04		Patients Signature Source Cd. - C	S		OI04		Not currently mapped - New constant - C
OI06		Release of Information Code - A	R		OI06		Not currently mapped - New constant - A
NM101	2330A	Entity Identifier Code - IL	R		NM101	2330A	Not currently mapped - New constant - IL
NM102		Entity Type Qualifier - 1	R		NM102		Not currently mapped - New constant - 1
NM103		Name Last / Org. Name	R		NM103		Not currently mapped, New field - Ins-Last-Name-2
NM104		Name First	S		NM104		Not currently mapped, New field - Ins-First-Name-2
NM105		Name Middle			NM105		
NM107		Name Suffix			NM107		
NM108		Identification Code Qualifier - MI	R		NM108		Not currently mapped, New constant - MI
NM109		Identification Code	R		NM109		Not currently mapped,

ADHS/DBHS				GREABHA		
						New field - Insureds-ID-Num-2
NM101	2330B	Entity Identifier Code - PR	R	NM101	2330B	Not currently mapped, New content - PR
NM102		Entity Type Qualifier - 2	R	NM102		Not currently mapped, New constant - 2
NM103		Name Last / Org. Name	R	NM103		Not currently mapped, New field - Payor-Name-2
NM108		Identification Code Qualifier - PI	R	NM108		Not currently mapped, New constant - PI
NM109		Identification Code	R	NM109		Not currently mapped, New field - Payor-Org-ID-2
LX01	2400	Assigned Number	R	LX01	2400	Memory Variable: LX01 : Assigned Number Counter
SV101		Composite Medical Proc. Id.	R	SV101		Composite Medical Proc. Id.
SV101-1		Product Service ID Qual. - HC	R	SV101-1		Product Service ID Qual. - HC
SV101-2		Product Service ID - Procedure Code	R	SV101-2		Procedure-Code
SV101-3		Procedure Modifier - Procedure Code Modifier	S	SV101-3		Modifier1
SV101-4		Procedure Modifier		SV101-4		
SV101-5		Procedure Modifier		SV101-5		
SV101-6		Procedure Modifier		SV101-6		
SV102		Monetary Amount - Line Item Charge Amt	R	SV102		Line-Charges
SV103		Unit or Basis For Meas. Code - UN	R	SV103		Unit or Basis For Meas. Code - UN
SV104		Quantity - Units	R	SV104		Units-Of-Service
SV105		Facility Code Value - POS	S	SV105		Place-Of-Service
SV107		Composite Diagnosis Cd. Pt	S	SV107		Composite Diagnosis Cd. Pt
SV107-1		Diagnosis Code Pointer	R	SV107-1		Diagnosis-Ptr1
SV107-2		Diagnosis Code Pointer	S	SV107-2		Diagnosis-Ptr2
SV107-3		Diagnosis Code Pointer	S	SV107-3		Diagnosis-Ptr3
SV107-4		Diagnosis Code Pointer	S	SV107-4		Diagnosis-Ptr4
SV109		Yes/No Condition Resp. Code - Y if emergency	R	SV109		Emergency-Ind
SV110		Yes/No Condition Resp. Code	S	SV110		
SV111		Yes/No Condition	S	SV111		

ADHS/DBHS				GREABHA		
		Resp. Code				
SV115		Copay Status Code	S	SV115		
DTP01	2400	Date/Time Qualifier - 472	R	DTP01	2400	Date/Time Qualifier - 472
DTP02		Date Time Period Form.Qual. - RD8	R	DTP02		Date Time Period Form.Qual. - RD8
DTP03		Date Time Period: CCYYMMDD-CCYYMMDD	R	DTP03		Memory Variable: Service Date: Service Date Concatenate
CN101	2400	Contract Type Code	R	CN101	2400	Currently not mapped
CN102		Monetary Amount	S	CN102		Currently not mapped
SE01		Number of Included Segments - Total Number of segments	R	SE01		Number of Included Segments - Total Number of segments
SE02		Trans. Set Control Number	R	SE02		

***Data Map* - NCPDP (Drug Claim)**

GREABHA has the ability to receive Drug Claims data via an NCPDP file. Following is the data map for the NCPDP file, specific to ADHS/DBHS:

ADHS/DBHS NCPDP				GREABHA		
Segment Name	**Field Name**	**Element ID**	**Location**	**Element Name**	**Description**	**Field Size**
Batch Header	RBHA ID from Header	N-4	880 - K1	Sender ID	Assigned Regional Behavioral Health Authority ID.	2
Batch Header	Transfer Date	N-6	800-K2	Creation Date	The date the file was produced.	8
Batch Header	Transfer Time	N-7	800-K3	Creation Time	The time the file was produced.	6
Batch Header	ADHS/BHS	N-10	800-K7	Receiver ID	Processor Defined Receiver ID	24
Detail Record	ICN number	N-14	880- K5	Transaction Reference Number	Invoice Control number ICN or claim number.	10
Transaction Header	ICN number	B1--14-4	104-A4	Processor Control Number	ICN Number (last 10 digits.)	11
Transaction Header	Provider ID qualifier	B1-14-6	202-B2	Service Provider ID Qualifier	Medicaid "5"	2
Transaction Header	NABP-ID & Location	B1-14-7	201-B1	Service Provider ID	AHCCCS Provider ID and Location for Pharmacy.	9
Transaction Header	Service Start Date	B1-14-8	401 - D1	Date of Service	Indicates the first date the service was provided.	8
Prescriber Segment	Prescriber ID qualifier	B1-14-13	466-EZ	Prescriber ID qualifier	Medicaid "05"	2

ADHS/DBHS NCPDP				GREABHA		
Segment Name	**Field Name**	**Element ID**	**Location**	**Element Name**	**Description**	**Field Size**
Prescriber Segment	Prescriber AHCCCS-ID & Location		411-DB	Prescriber ID	Prescriber AHCCCS-ID & Location.	9
Insurance Segment	Client ID	B1-14-19	302-C2	Cardholder ID	Unique 10 digit ID alphanumeric field. Auto generated by CIS.	10
Insurance Segment	RBHA ID	B1-14-21	301-C1	Group ID	Assigned Regional Behavioral Health Authority ID.	2
Claim Segment	NCD Code	B1-14-32	407-D7	Product/Service ID	Valid NCD code.	19
Claim Segment	Modifier	B1-14-36	459-ER	Procedure Modifier Code	Procedure Modifier Code (spaces.)	2
Claim Segment	Dispense Qty	B1-14-38	442-E7	Quantity Dispensed	Number of doses dispensed.	10
Claim Segment	Number this Refill	B1-14-40	403-D3	Fill Number	Number of refills authorized. Default value is 00.	2
Claim Segment	Rx Order Date	B1-14-42	414-DE	Date Prescription Written	The date the RX was written.	8
Claim Segment	Refills Authorized	B1-14--44	415-DF	Number of refills authorized	Default value is 00.	2
Claim Segment	Days Supply	B1-14-46	405-D5	Days Supply	Days Supply.	3
Pricing Segment	Ingredient Cost	B1-14-66	409-D9	Ingredient Cost	See overpunch information.	8
Pricing Segment	Dispensing Fee	B1-14-68	412-DC	Dispensing Fee	Dispensing Fee. See overpunch information.	8
Pricing Segment	Co-Pay Amount	B1-14-70	433-DX	Patient Paid Amount	Patient co-payment amount. See overpunch information.	8
Pricing Segment	Prescription Cost	B1-14-72	430-DU	Gross Amount Due	Amount Paid on prescription. See overpunch information.	8

3.3. Other File Formats

Due to the HIPAA standards, Centene modified its internal processes, procedures and file layouts in order to produce ANSI transaction sets. Due to these modifications, those business partners who receive electronic files from Centene will be required to modify their current applications in order to incorporate the new file layouts either in the HIPAA mandated transaction set or the proprietary file.

Centene business associates who are considering themselves as a “non-covered entity” under the HIPAA guidelines will not be required to receive information in the HIPAA ANSI transaction sets. For this reason, Centene will supply those business associates with a new proprietary file layout for the matching HIPAA ANSI transaction set. In some instances, a proprietary file may not be available for a particular HIPAA ANSI transaction set.

GREABHA will also support ADHS/DBHS with the following data file exchanges:

- TPL
- Grievance and Appeals Data Submission
- Eligibility Inquiries (270/271 Transactions) daily
- AHCCCS Eligibility Application Status Reports
- Eligibility Outbound

Eligibility Outbound

The Eligibility Outbound proprietary file will contain all eligible members at the time the file was processed. Any member who is not sent on this file but was sent on a previous file is considered on hold or terminated. Centene can provide a supplemental “change” file upon request. This change file will contain the members that had a record change that resulted in a new member span. These files will be available for receipt approximately the same time each month, and partners will be notified immediately if there are any changes to the schedules.

Field #	Field Name	Type	Field Length	Position		Req	834 Element ID	NOTES
				From	Thru			
01.0	Record Type	X	1	001	001	Req		"H" Record type header
02.0	Plan Name	X	30	002	031	Req		Name of the plan that generates the file.
03.0	File Date	X	8	032	039	Req		Date the file is generated.
01.0	Record Type	X	1	001	001	Req		"D" Record type detail
02.0	Transaction Set Ref	X	29	002	030	Req	BGN02	Trading Partner ID + Region
03.0	Transaction Date	X	8	031	038	Req	BGN03	
04.0	Transaction Time	X	8	039	046	Req	BGN04	
05.0	Master Policy Number	X	30	047	076	Req	REF02	Trading Partner ID + Region
06.0	Date Time	X	8	077	084	Req	DTP03	
07.0	Insurer Name	X	30	085	114	Sit	N102	
08.0	Insurer ID Code	X	10	115	124	Req	N104	
09.0	Insured Death Date	X	8	125	132	Sit	INS12	If not applicable, this will be space filled.
10.0	State Assigned	X	14	133	146	Req	REF02	REF01 = "0F"

Field #	Field Name	Type	Field Length	Position		Req	834 Element ID	NOTES
				From	Thru			
	Member Number							
11.0	Policy Number	X	12	147	158	Req	REF02	REF01 = "ZZ"
12.0	Case Number	X	12	159	170	Sit	REF02	REF01 = "3H"
13.0	Eligibility Begin Date	X	8	171	178	Req	DTP03	DTP01 = "356"
14.0	Eligibility End Date	X	8	179	186	Req	DTP03	DTP01 = "357"
15.0	Member Last Name	X	14	187	200	Req	NM103	
16.0	Member First Name	X	14	201	214	Req	NM104	
17.0	Member Middle Name	X	1	215	215	Sit	NM105	
18.0	Identification Code Qualifier	X	2	216	217	Sit	NM108	NM108 = "34"
19.0	Mbr SSN#	X	12	218	229	Sit	NM109	Auto filled with 9 nines if the SSN# is absent.
20.0	Member's Telephone Number	X	20	230	249	Req	PER04	
21.0	Member Address Line 1	X	36	250	285	Req	N301	
22.0	Member Address Line 2	X	36	286	321	Sit	N302	
23.0	Member City Name	X	24	322	345	Req	N401	
24.0	Member State Code	X	2	346	347	Req	N402	
25.0	Member Zip Code	X	10	348	357	Req	N403	
26.0	Member County Code	X	30	358	387	Sit	N406	Member County Code + Risk Pop. (The + will not be included).
27.0	Member Birth date	X	8	388	395	Req	DMG02	
28.0	Gender Code	X	1	396	396	Req	DMG03	
29.0	Provider Last Name	X	14	397	410	Req	NM103	
30.0	Provider First Name	X	14	411	424	Req	NM104	
31.0	Provider ID	X	10	425	434	Sit	NM108	
32.0	Business Unit	X	2	435	436	Req	REF02	REF01 = "DX"
33.0	Carrier	X	2	437	438	Req	REF02	REF01 = "DX"
34.0	Program Number	X	2	439	440	Req	REF02	REF01 = "DX"

Field #	Field Name	Type	Field Length	Position		Req	834 Element ID	NOTES
				From	Thru			
35.0	Region	X	2	441	442	Req	REF02	REF01 = "DX"
36.0	Division Number	X	10	443	452	Req	REF02	REF01 = "DX"
37.0	Group Number	X	6	453	458	Req	REF02	REF01 = "IL"
38.0	Employee Status	X	2	459	460	Req	REF02	REF01 = "ZZ"
39.0	Health Status	X	2	461	462	Req	REF02	REF01 = "ZZ"
40.0	Contract Type	X	2	463	464	Req	REF02	REF01 = "ZZ"
41.0	Pharmacy Indicator 1	X	15	465	479	Req	REF02	REF01 = "17"
42.0	Pharmacy Indicator 2	X	15	480	494	Req		REF01 = "17"
43.0	Filler	X	145	495	639	Req		
01.0	Record Type	X	1	001	001	Req		"T" Record type trailer
02.0	Plan Name	X	30	002	031	Req		Name of the Plan that generates the file.
03.0	File Date	X	8	032	039	Req		Date the file is generated.
04.0	Record Count	X	8	040	047	Req		Total number of records in the file.

4. Establishing Exchange Capabilities

In order to establish exchange capabilities with GREABHA, the relationship must be formally established through the process identified in this sub-section.

4.1. Trading Partner Profile

Anyone wanting to exchange information electronically with GREABHA must first complete and submit a Trading Partner Profile. A trading partner is an entity with whom an organization exchanges data electronically. The trading partner may send or receive information electronically. This includes but is not limited to Providers and third parties such as Clearinghouses, Value Added Network (VAN), Billing Service, Coordination of Benefits (COB) provider, Software Vendors, Application Development organizations, etc.

Once testing is successfully completed, the Provider and/or Third Party will receive written notice of approval via e-mail or mail. The Third Party must provide this notice to clients or providers, who in turn must provide appropriate software vendor information on their trading partner profile.

A sample Trading Partner Profile is provided below:

TRADING PARTNER PROFILE

Centene Corporation is a fully integrated multi-state government services managed care company. The Company's government services market includes Medicaid, SCHIP and SSI. The Company operates plans in Indiana, New Jersey, Ohio, Texas, and Wisconsin. For the purposes of this Trading Partner Agreement, when "Centene" is used going forward, it applies to all Health Plans on this Trading Partner Profile form.

COMPANY INFORMATION	
Name	
Address	
City, State and Zip	
Contact Name	
Contact Phone Number	
Contact Fax Number	
Contact E-Mail Address	

CLEARINGHOUSE/INTERMEDIATE SERVICE INFORMATION (if applicable)	
Company Name	
Address	
City, State and Zip	
Contact Name	
Contact Phone Number	
Contact Fax Number	
Contact E-Mail Address	

MEDICAL SOFTWARE USED INTERNALLY (if applicable)	
Software Name	
Company Name	
Address	
City, State and Zip	
Contact Name	
Contact Phone Number	
Contact Fax Number	
Contact E-Mail Address	

SENDER/RECEIVER ID'S	
Sender ID (ISA06/GS02)	
Receiver ID (ISA08/GS03)	

1

INBOUND ELECTRONIC TRANSACTION SETS (please mark all that apply) These are transactions sets that you are planning to submit to Centene. Centene will always send a 997 Functional Acknowledgement back to the sender confirming receipt.	
HIPAA	
☐	ANSI X12N 270 – Health Plan Eligibility – Solicitation
☐	ANSI X12N 276 – Health Claim Status – Solicitation
☐	ANSI X12N 278 – Referral Certification and Authorization
☐	ANSI X12N 820 - Health Plan Premium Payments
☐	ANSI X12N 834 - Enrollment/Disenrollment in a Health Plan
☐	ANSI X12N 835 – Claim Payment and Remittance Advice
☐	ANSI X12N 837 – Healthcare Claim or Encounter – Dental
☐	ANSI X12N 837 – Healthcare Claim or Encounter – Institutional
☐	ANSI X12N 837 – Healthcare Claim or Encounter: Professional
PROPRIETARY	
☐	Healthcare Encounter – Dental
☐	Healthcare Encounter – Institutional
☐	Healthcare Encounter – Professional

2

OUTBOUND ELECTRONIC TRANSACTION SETS (please mark all that apply) These are transactions sets that you would like to receive from Centene.	
HIPAA	
☐	ANSI X12N 271 – Health Plan Eligibility – Response to Solicitation
☐	ANSI X12N 277 – Health Claim Status – Response to Solicitation
☐	ANSI X12N 278 – Referral Certification and Authorization
☐	ANSI X12N 820 - Health Plan Premium Payments
☐	ANSI X12N 834 - Enrollment/Disenrollment in a Health Plan
☐	ANSI X12N 835 – Claim Payment and Remittance Advice
☐	ANSI X12N 837 – Healthcare Claim or Encounter – Dental
☐	ANSI X12N 837 – Healthcare Claim or Encounter – Institutional
☐	ANSI X12N 837 – Healthcare Claim or Encounter: Professional
PROPRIETARY	
☐	Eligibility Enrollment Roster

TAX ID'S Please list all Tax IDs that you will be billing under			

4.2. Trading Partner Agreement

Prior to going "live" with the first electronic transaction, a signed Trading Partner Agreement must be received by GREABHA. This applies to Providers or any Third Party acting on the Providers behalf, which are submitting transactions directly to GREABHA.

A sample Trading Partner Agreement is provided below:

Trading Partner Agreement

This Trading Partner Agreement (hereinafter "Agreement") is made by and between Centene Corporation ("Centene") d/b/a Cenpatico Behavioral Health ("GREABHA") and "Provider", a licensed health care provider or a Trading Partner.

WHEREAS, Centene performs certain claims processing and administrative services; and,

WHEREAS, Provider renders certain professional health care services ("Services") to members and individuals, and submits documentation of those Services to Centene; and,

WHEREAS, Provider and Centene (collectively, the "Parties") desire to exchange by and through electronic communications, certain claims and billing information, membership, authorization and referrals, that may contain identifiable financial and/or protected health information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 Code of Federal Regulations Parts 160-164, and applicable regulations that implement Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq. (the "GLB Regulations") now or as later amended; and,

WHEREAS, the Parties agree to safeguard any and all PHI or other Data received, transmitted or accessed electronically to or from each other in accordance with HIPAA and the GLB Regulations, and desire to set forth in writing their understanding with respect to these communications and the covenant of confidentiality and non-disclosure of PHI or other Data.

NOW THEREFORE, in consideration of the mutual promises and covenants contained herein and other good and valuable consideration, the receipt of which is hereby acknowledged, the Parties hereto agree as follows:

I. DEFINITIONS

Data. Any information provided and/or made available by either of the Parties to the other, and includes, but is not limited to enrollment and eligibility data, claims data, and PHI.

Implementation Guide. A technical user's manual provided to Provider to assist Provider in preparing and completing electronic data interchange. Centene reserves the right to revise and update the Implementation Guide ("Guide") in its sole discretion.

Health and Human Services ("HHS") Privacy Standard Regulation. 45 Code of Federal Regulations ("CFR") at Title 45, Parts 160 through 164.

HHS Transaction Standard Regulation. 45 CFR Parts 160 and 162.

Individual. The person who is the subject of the Data, as defined by 45 CFR § 164.501.

Proprietary Data. That information used in Centene's business or business practices to which Provider would not otherwise have access but for its contractual relationship with Centene, including but not limited to information systems technologies and practices, and operational processes.

II. INTRODUCTION

This Agreement authorizes the Parties to electronically exchange Data, including PHI, through a public or private telecommunications network using language and code sets authorized at 45 CFR § 160 et seq., in an efficient and cost-effective manner without limiting the obligations of each party as set forth in this Agreement or imposed by applicable law, solely for the purposes set forth herein, in accordance with the terms "Standard" and "Transactions" as defined at 45 CFR § 160.103 (hereinafter aggregated and referred to as "Standard Transactions"), the privacy standards described and referenced below, and requirements for non-standard transactions (if applicable). Any Data, Proprietary Data or PHI exchanged under this Agreement is to be used and exchanged solely as authorized by HIPAA, and is further subject to the terms and conditions set forth in this Agreement.

III. TERM, TERMINATION and SUSPENSION

The term of this Agreement shall commence upon its execution. Provider agrees that its ability to transmit, receive or otherwise electronically access Data will cease if Provider or Centene terminates this Agreement. Either party may terminate this Agreement without cause upon sixty-(60) days written notice or immediately by either party for cause. Cause shall include, but not be limited to, breach of any material term(s) of this Agreement, fraud, abuse, and/or failure to protect PHI. The terminating party may rescind notice of termination if the other party successfully cures the breach complained of to the terminating party's satisfaction. Each party may also temporarily suspend electronic communications under this Agreement to protect computer or data systems in cases of emergencies, or to perform maintenance. Each party agrees to minimize the frequency and duration of these temporary suspensions.

IV. Centene OBLIGATIONS

A. **ID(s) and Password(s)**. Upon execution of this Agreement, Centene will assign logon ID(s) and password(s) to Provider to allow Provider to authenticate its identity and transmit data electronically. Centene shall retain title to all logon ID(s) and password(s), and reserves the right to change any logon ID or password at any time, for any reason, or if required to do so by law, regulation, or court order.

B. **Data**. The Data the Parties may exchange pursuant to this Agreement may change as a result of changes in law or regulation, or actions taken in accordance with the terms and conditions of certain health care benefits contracts, or changes made to those contracts. Centene does not warrant the accuracy or completeness of the Data it sends to Provider; acceptance by Centene of the Data Provider sends electronically does not constitute guarantee of reimbursement.

V. PROVIDER OBLIGATIONS and AUTHORIZATIONS

C. **Provision of Data.** Provider may provide Centene Data electronically, including the minimum necessary PHI (see 45 CFR § 164.502(b)) in accordance with the terms of the

Agreement and the Guide. Provider is solely responsible to ensure that the Data it provides Centene is correct.

D. **Logon ID and Password**. Provider agrees to protect Centene's logon ID(s) and password(s) from compromise, release or discovery by any unauthorized person, and shall not disclose logon ID(s) and password(s) to any third party in any manner. If a breach of this provision occurs, Provider must notify Centene immediately as set forth in the Guide. Provider acknowledges and agrees that only Provider personnel it designates shall be permitted to use the logon ID(s) and password(s), and that Provider shall designate only such individuals as who have a need to use the logon ID (s) and password(s) in connection with the legitimate business needs of Provider as they relate to the underlying business relationship between Provider and Centene. Provider's use of logon ID(s) and password(s) constitutes an Electronic Signature that confirms Provider's willingness to: remain bound by these terms and conditions and ratify any transaction conducted electronically by Centene. Provider agrees that Provider is solely responsible for the use of the Provider's logon ID(s) and password(s) by another party, except to the extent due to the negligence of Centene.

E. **Provider's Costs.** Provider shall assume all its internal costs to transmit, access and receive Data electronically including, but not limited to, the costs of computers, terminals, connections, modems, and browsers that have the capability to use HIPAA-mandated code-set Standard Transactions, and the costs of providing sufficient security measures to safeguard receipt and transmission of PHI in accordance with 42 USC § 1320d-2(d), 45 CFR § 164.530 and the implementing regulations issued by HHS to preserve the integrity and confidentiality of, and to prevent non-permitted use or violations of disclosure of PHI. Provider acknowledges that any changes made to Data may impact any reimbursement it receives. Provider shall be responsible for regularly backing up Data and for maintaining adequate records to enable Provider to replicate Data transmitted pursuant to this Agreement.

F. Authorization to Use Data. Provider's use of a Centene system or process under this Agreement constitutes authorization and direction to Centene to use PHI or other Data to adjudicate and process health care claims Centene receives from Provider. Provider may access, receive and transmit only that Data in such format as described in the Guide. No electronic communication will give rise to any obligation until it is accessible at the receiving party's computer as set forth in the Guide. Provider acknowledges that Centene may disclose the PHI it makes available to Centene concerning Individuals who are members of a plan to the plan sponsor consistent with HIPAA's requirements and the language set forth herein.

G. Proprietary Information. Provider covenants that it will not, either during or after the term of this Agreement, disclose any Proprietary Information to any third party for any reason whatsoever, except to officers, directors, employees and agents of Provider who have a need to know the Proprietary Information in connection with the performance of the parties' obligations under this or other agreements between the parties, and, except as contemplated under the terms of this Agreement, to not use Proprietary Information without the prior written authorization of Centene, unless such information is in the public domain through no fault of Provider, or except as may be required by law, provided Provider promptly furnishes prior written notice of such required disclosure to Centene and cooperates with Centene in taking such steps as are legally available to prevent such disclosure or to cause such disclosure to be made in such a manner as to protect the confidential nature thereof.

H. Representations and Warranties. Provider hereby represents and warrants to Centene that Provider has never been, for any period of time, excluded from, or in any way sanctioned by, the Medicare or Medicaid programs or any other federal or state health care program. Provider agrees that he shall notify Centene within five (5) days of receipt

of an initial sanction notice, notice of proposed sanction, or notice of the commencement of a formal investigation, or the filing of charges by a Medicare peer review organization, the Department of Health and Human Services, or any law enforcement agency or health regulatory agency of the United States or any state.

VI. INDEMNIFICATION

Each party shall release, defend, indemnify and hold harmless the other party, its corporate subsidiaries, affiliates officers, directors, employees, agents, persons, firms, divisions, successors and assigns, against any and all: liability, losses or damages, whether direct or indirect, to person or property; claims; judgments; costs and reasonable attorney's fees; legal action or potential for the same which may result from the improper use or unauthorized disclosure or use of Data or PHI in violation of this Agreement by the first party or any employee or agent thereof. Each party assumes all liability for any damage, whether direct or indirect, to the Data or the other party's information systems caused by the unauthorized use of such Data or information systems by the first party, its employees or agents or any third party who gains access to the systems through their acts or omissions. Neither party shall be liable to the other party for damages caused by circumstance beyond its control, including, without limitation: "hackers" who gain access to the system or Data in spite of a party's compliant security measures, a major disaster, epidemic, the complete or partial destruction of its facilities, riot, civil insurrection, war or similar causes. Neither party shall be liable to the other party for any special, incidental, exemplary or consequential damages. Each party shall obtain and maintain at its sole expense, and in amounts consistent with industry standards, insurance to support its indemnification obligations under this Section, and shall supply proof of such insurance to the other upon request.

VII. COMPLIANCE WITH PRIVACY STANDARDS

Each party will develop, implement, maintain and use appropriate administrative, technical and physical Data safeguards, in compliance with 42 U.S.C. § 1320d-2(d), 45 CFR § 164.530(c) and patient confidentiality provisions of applicable state statutes or regulations, and shall comply with any applicable GLB Regulations, or any amendments to any of these statutes or regulations.

Each party shall execute trading partner, and/or business associate agreements with subcontractors or agents that provide services involving maintenance, use or disclosure of PHI, ensuring that any subcontractors or agents to whom it provides PHI agree in writing to those restrictions that, with respect to such PHI, apply to that individual subcontractor or agent pursuant to this Agreement. Each party agrees that it will not maintain, use, make available or further disclose PHI other than as permitted or required by this Agreement or as required by law.

If any activity under this Agreement would cause any Party to be considered a "Business Associate" of any other Party under 45 CFR. § 160.103, the following restrictions will apply to all uses and disclosures of PHI. The Business Associate will: (i) Not use or further disclose PHI other than as permitted or required by this Agreement, or to comply with judicial process or any applicable statute or regulation; (ii) Notify the other Party in advance of any disclosure of PHI that the Business Associate is required to make under any judicial or regulatory directive; (iii) Use appropriate safeguards to prevent use or disclosure of PHI other than for the purposes required in this Agreement; (iv) Report to the other parties any use or disclosure of PHI not provided for in this Agreement of which the Business Associate becomes aware; (v) Ensure that any agents or subcontractors to whom the Business Associate discloses PHI received from another party, or created on behalf of another party, agree to the same restrictions and conditions that apply to the protection of information under this Agreement; (vi) Make PHI available to individuals as required by 45 CFR § 164.524; (vii) Make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 CFR § 164.526; (viii) Make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528; (ix) Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or collected by the Business Associate on behalf of another Party, available to the Secretary of HHS when called upon for purposes of determining the other Party's compliance with federal

privacy standards; and (x) At termination of this Agreement, if feasible, return or destroy all PHI received from another Party, or created or collected by the Business Associate on behalf of the other Party, that the Business Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, or if the PHI is still used to perform business functions, continue to treat all such PHI in accordance with the limits provided in this Agreement, and applicable law and regulation. This paragraph shall have no effect and shall not apply to the parties to the extent a written Business Associate Agreement has already been executed and is in effect between the parties, in which case the terms of such Business Associate Agreement will apply instead.

VIII. SYSTEMS AND PERSONNEL SECURITY/UNAUTHORIZED DISCLOSURES.

The Parties shall comply with the final version of the data security standards published by HHS on February 20, 2003 and found at 45 CFR Parts 160, 162 and 164, 68 Federal Register, Pages 8333-8399 (the "Security Standard"). On or before April 21, 2005, the required compliance date of the final Security Standard, the Parties will adopt any necessary modifications to their practices for maintaining PHI or transmitting PHI electronically, and shall provide any written assurances, as required under the final Security Standard. If an unauthorized disclosure of PHI, or the discovery of unauthorized access to and/or tampering with the Data or Centene's Proprietary Data is discovered, the disclosing party will immediately report to the other party, using the most expeditious medium available, no later than twenty-four (24) hours after such discovery/disclosure is made, the following information: (i) the nature of the disclosure, (ii) PHI used or disclosed, (iii) the individual(s) who made and received the disclosure, (iv) any corrective action taken to prevent further disclosure(s) and mitigate the effect of the current disclosure(s), and (v) any such other information reasonably requested by the non-disclosing party. The Parties will cooperate in the event of any litigation concerning unauthorized use, transfer or disclosure of such Data.

IX. COMPLIANCE WITH STANDARD TRANSACTIONS

When required, the Parties shall comply with each applicable regulation when performing "Standard Transactions." The Parties will not enter into any Trading Partner Agreement related to this Agreement that: changes any definition, data condition or use of a data element or segment, nor adds any data elements or segments to the maximum defined data set as proscribed in the HHS Transaction Standard Regulation, and as further proscribed by Centene. The Parties further agree that they will neither use any code or data elements marked “not used” or which are not found in the HHS Transaction Standard’s implementation specifications, nor change the meaning or intent of any of the HHS Transaction Standard implementation specifications. (See 45 CFR § 162.915).

X. NOTICES

Any notice relating to this Agreement shall be in writing and transmitted by either (i) U.S. Mail, first class, postage prepaid; or (ii) facsimile transmission with transmission acknowledgment received by the facsimile sender, provided written notice delivered by the means of delivery specified in subsection (i) of this Section follows such facsimile; or (iii) e-mail, to the addresses/telephone numbers/e-mail addresses contained in the Guide, provided written notice delivered by the means of delivery specified in subsection (i) of this Section follows such e-mail. Notices or communications shall be deemed given (a) in the case of transmittal by U.S. mail, on the date of receipt by the addressee and (b) in the case of e-mail or facsimile transmission, on the date the e-mail or facsimile is sent.

XI. RECORDS AND AUDIT

The Parties shall maintain, in accordance with their document retention policies and applicable law and regulation, and for a minimum of seven (7) years, true and correct copies of any source documents (e.g., medical records) from which they reproduce Data. Centene reserves the right to

audit those records and security methods of Provider necessary to ensure compliance with this Agreement or to ensure that adequate security precautions have been taken to prevent unauthorized disclosure of any Data.

XII. SURVIVAL OF PROVISIONS

Any provision of this Agreement which requires or reasonably contemplates the performance or existence of obligations by either party after the termination of the Agreement shall survive such termination.

XIII. ASSIGNMENT

No right or interest in this Agreement shall be assigned by either party without the prior written permission of the other party.

XIV. GOVERNING LAW

The construction, interpretation and performance of this Agreement and all transactions under it shall be governed by the laws of Missouri, except to the extent such laws are preempted by federal law.

XV. WAIVER OF RIGHTS

No course of dealing or failure of either party to strictly enforce any term, right or condition of the Agreement shall be construed as a waiver of such term, right or condition.

XVI. SEVERABILITY

If any provisions of this Agreement shall be deemed invalid or unenforceable, such invalidity or unenforceability shall not invalidate or render unenforceable the entire Agreement, but rather the entire Agreement shall be construed as if not containing those invalid or unenforceable provision(s), and the rights and obligations of each party shall be construed and enforced accordingly.

XVII. ENTIRE AGREEMENT

This Agreement and any Manuals, Guides, Exhibits and Attachments thereto shall constitute the entire Agreement between the Parties with respect to the subject matter of this Agreement and shall not be altered, varied, revised or amended except in writing signed by both Parties. In the event of any inconsistency between the provisions of this Agreement and those of any Guide, Exhibit or Attachment thereto, the terms of this Agreement shall prevail. Except as otherwise provided herein, the provisions of this Agreement shall supersede all prior oral or written quotations, communications, agreements and understandings of the Parties with respect to the subject matter of this Agreement.

BY SIGNING BELOW, the individual with authority to bind each of party is representing that he/she has read the foregoing Agreement and agrees on behalf of the party it represents to be bound by it. For purposes of this Agreement, an electronic signature shall have the full force and legal effect of an original signature.

PROVIDER

By: _____ _____

(Provider Signature) (Printed name)

_____ _____

(Title) (Date)

_____

(Business/Provider Name)

Centene CORPORATION

By: _____ _____

(Signature) (Printed name)

_____ _____

(Title) (Date)

4.3. Testing

Once we have received the completed Trading Partner Profile and signed Trading Partner Agreement, there are three levels of transaction testing required before an application is considered approved. These testing levels include the following:

- Compliance Testing
- Centene Specification Validation Testing
- End-to-End Testing

Centene requires a minimum of a three week testing cycle to include sending four test files containing “live” information to its’ business partners in the same manner as production files would be sent. This will allow us to test the file transmission process and the data content. Those four files will contain multiple scenarios depending on the type of transaction being sent. Additional testing required by ADHS/DBHS can be coordinated provided the appropriate and necessary lead time is given.

Once both Centene and ADHS/DBHS or its designated providers have approved the transaction, we will work together on setting up a timeframe to implement it into production.

5. Ad Hoc Electronic Data Requests

As mentioned previously, GREABHA will respond to ad hoc electronic data requests within the 30 day timeframe required if awarded this contract.

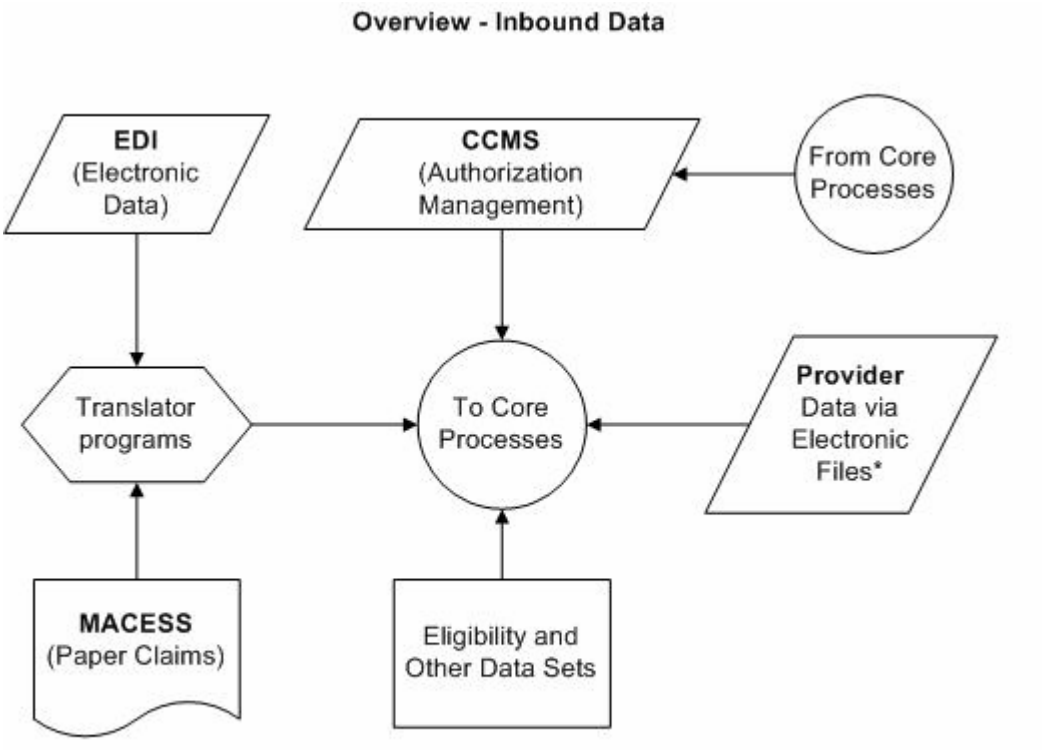
k. System Data Flow

1. Overview

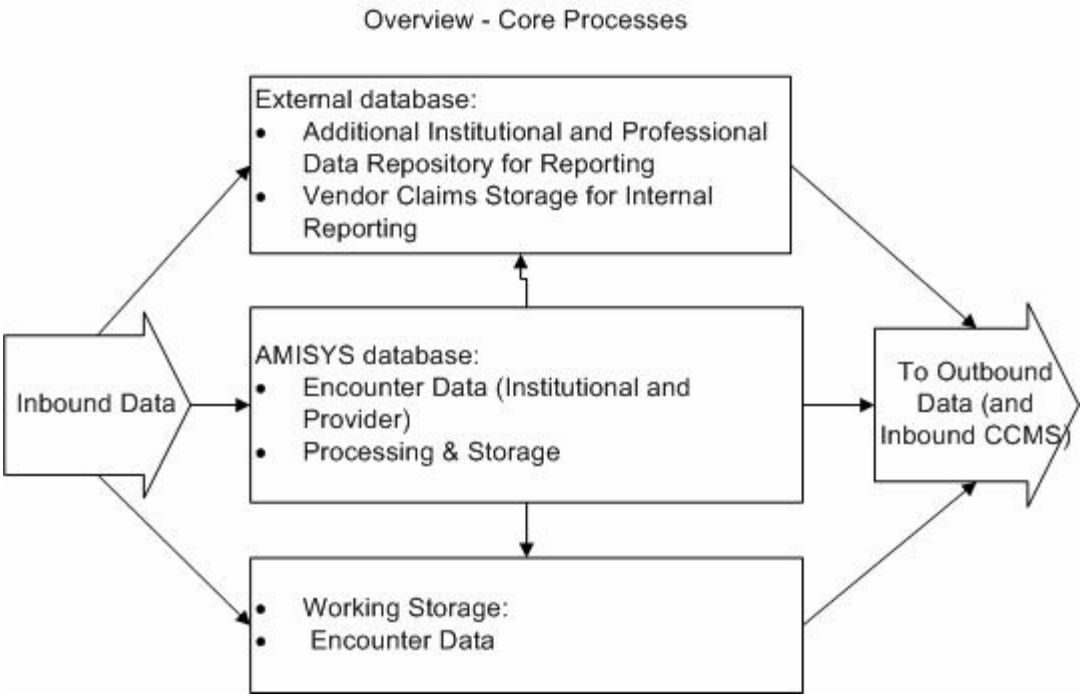
As previously discussed, Centene's core system for encounter / claims processing is AMISYS, which is housed on the HP 9000 machine. In addition to AMISYS, a number of interface processes have been built to attach to AMISYS and other external dataset structures to maintain our managed care business. Vendor related processing is also maintained through the HP 9000 environment. This overview section provides an outline of the inbound, core and outbound data flows, while detailed explanations of these processes and their linkage within the System Architecture and AMISYS are outlined further below.

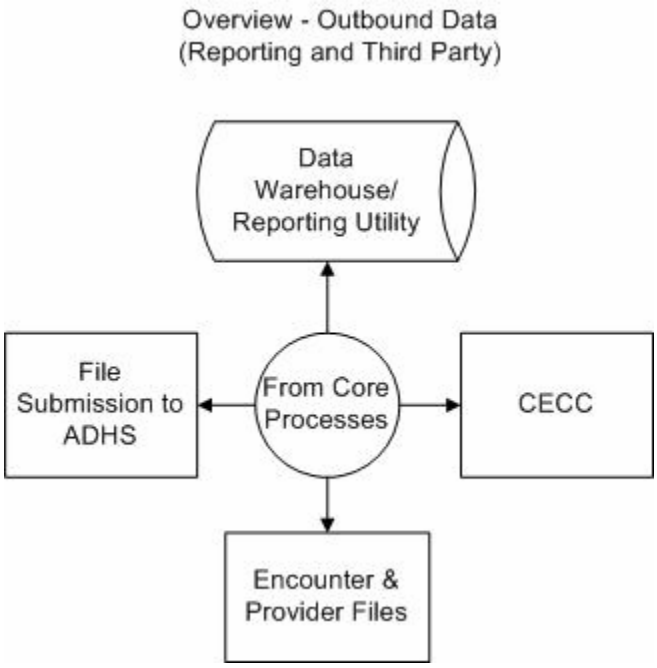
Data is maintained within AMISYS and all external datasets indefinitely, whether online or stored at an off-site facility. Data set structures are built to maintain history for claims, consumers, providers, authorizations and many other transactions. Retroactive adjustments to each of the datasets are kept online for historical review. A date spanning process is used to capture historical records such as Provider Contracting arrangements. AMISYS has a separate data set built just for auditing purposes. This dataset is built for redundancy and transactional tracking purposes.

The following MIS System Flow Diagrams overview the distinct inbound links, core systems and outbound or third party processing and reporting links:



* Data is received via FTP site pickup, Internal Bulletin Board drop off, or Secure Email Transmission.



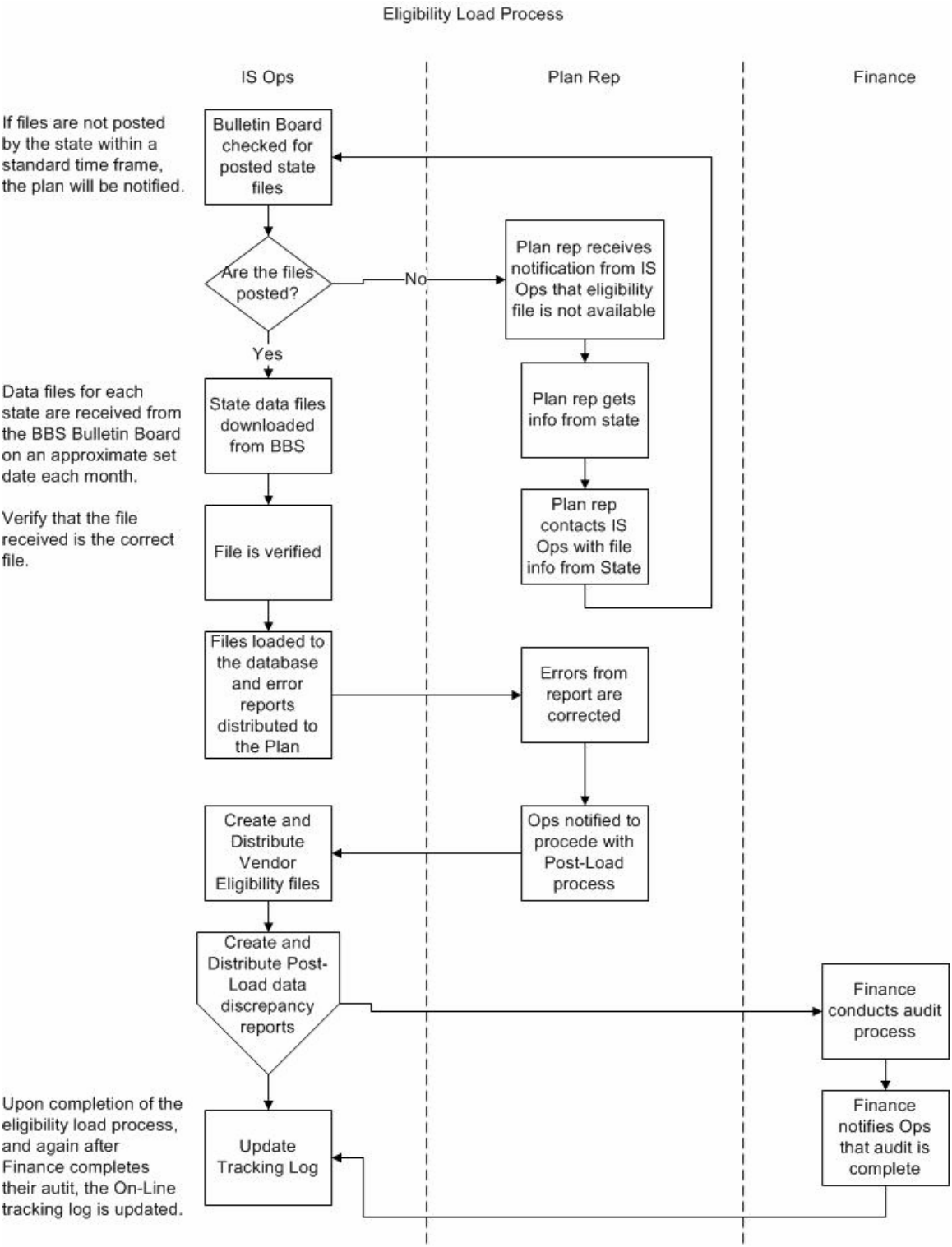


2. Membership - Enrollment/Eligibility

As previously discussed, the MIS department has created mapping/translation programs for loading membership, ultimately linking consumer eligibility status to all AMISYS subsystems. The mapping programs take the eligibility files, validate each data item and map each data item to the AMISYS standard membership batch input file format. Centene then uses the batch membership

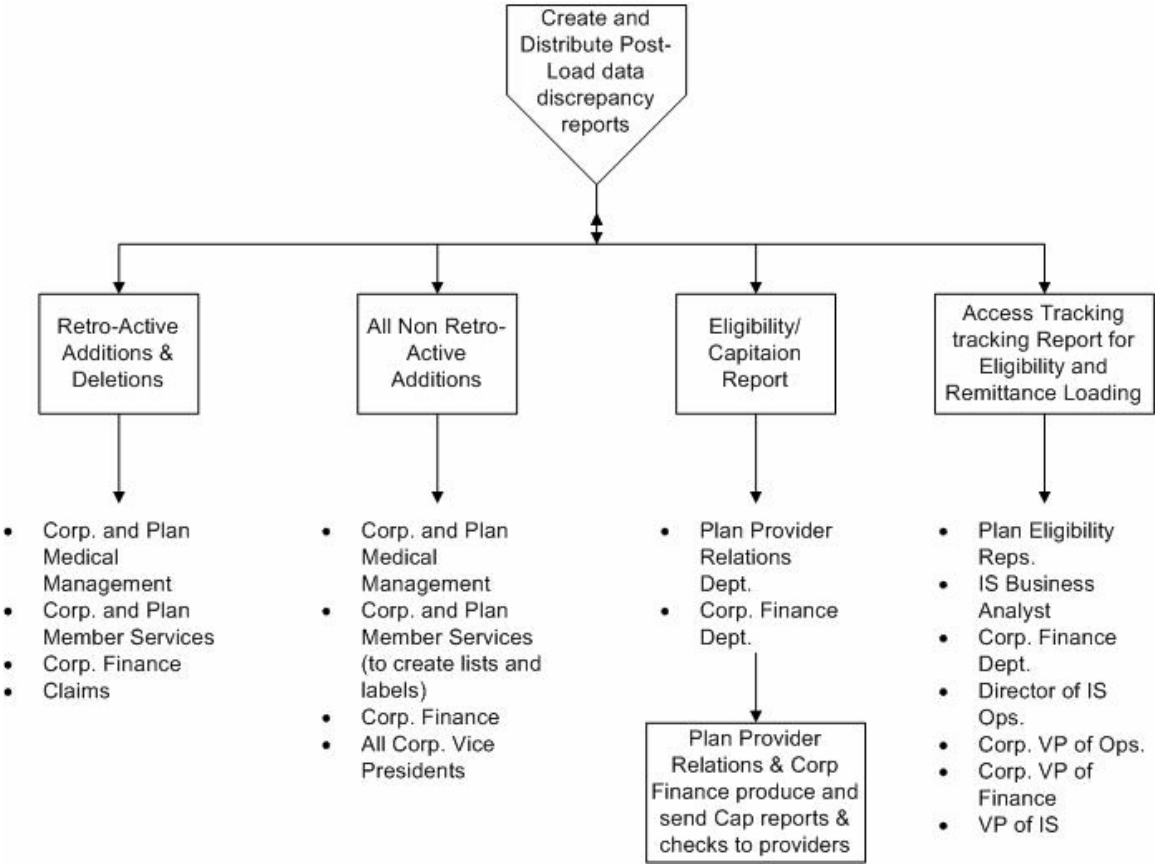
interface subsystem to further validate, cross-check and load the membership data into the main AMISYS tables, where the data is accessible from all subsystems. To increase operational efficiencies, the batch load process identifies possible duplicate consumers, as well as other errors and warnings, and produces an error report.

The following diagram illustrates the process performed to load the eligibility data files into the database, including all the validation processes supported:



As indicated on the eligibility load process flow, various discrepancy reports are prepared and distributed to validate an accurate load.

The following diagram illustrates the many reports and areas performing the reviews:



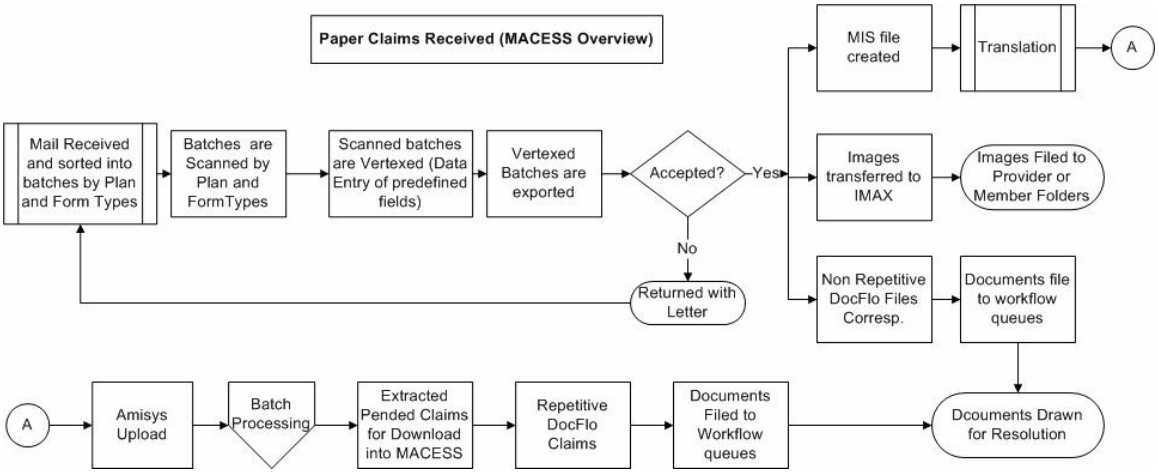
3. Claims Processing

The claims process has been discussed in various previous sections of this document, including the manual/batch process outlined in Section C, System Compatibility, and the EDI process in Section C, E, Ability to Provide a Secure Electronic Data Interface. The following diagrams and descriptions focus on the data flow and verification processes used to support the entire claims process.

3.1. Front-End Processing – Paper, Batch, EDI

Claims are received in two main forms, either Paper or Electronic. HCFA and UB claims received by paper are directed through our MACESS process flow. Once claims are sorted and batched they are ready for the vertexing or scanning and data entry process. Claims that are batched are available for entry through the vertex process. This high speed OCR/data entry process is highly efficient. Once claims are entered they are ready for processing through the translation programs or routed to reject queues where letters communicate the specific edit that did not pass in our upfront processing.

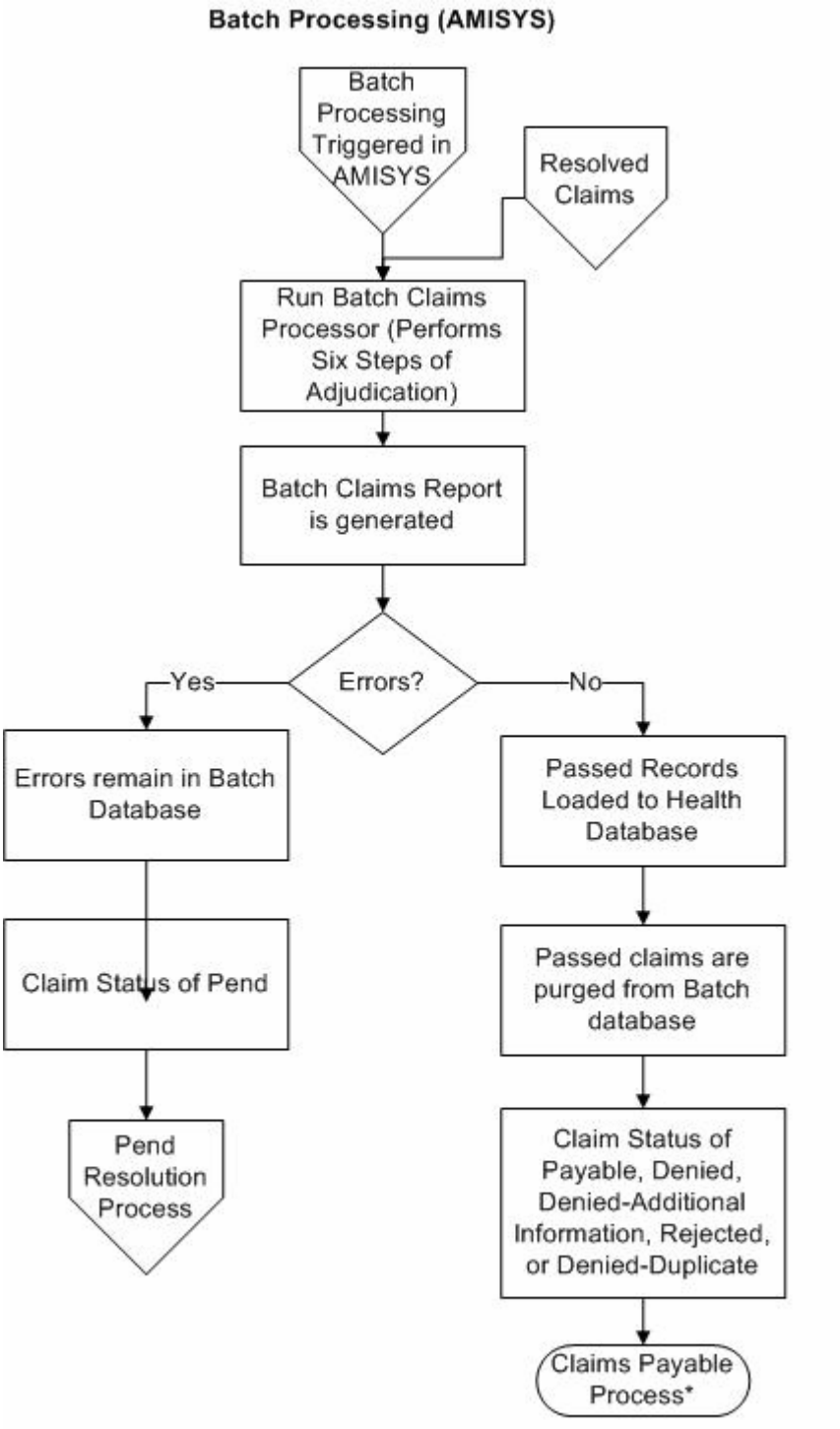
The following diagram illustrates this processing of paper claims:



Centene also accepts electronic claims data either directly from a provider, or through our clearinghouse relationships, as described in Section E, Ability to Provide a Secure Electronic Data Interface.

Once both Paper and EDI claims are processed through the translation programs, they are loaded into the Batch Database in AMISYS.

The following diagram illustrates the batch process:

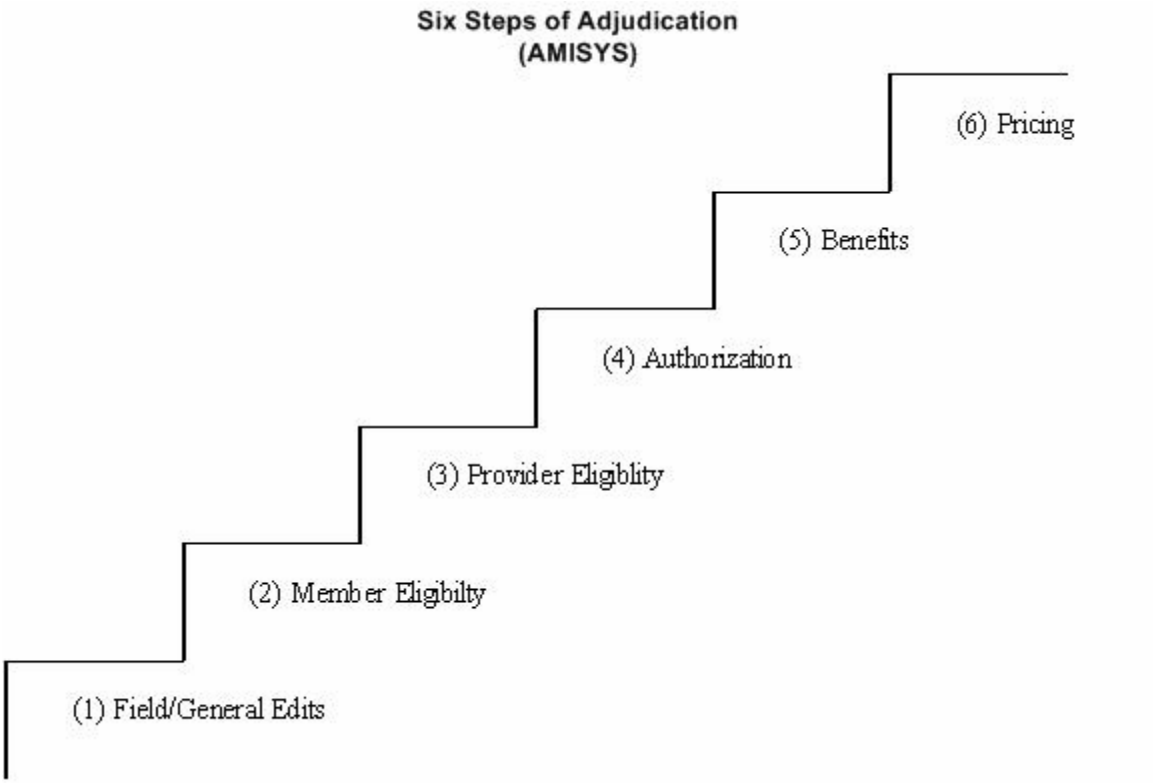


* Claims payable process can include payment to provider on payable claims as a service contracted accordingly with Centene.

3.2. Adjudication Process

As seen in the Batch processing diagram, the claims adjudication process is performed in six steps. These steps form a hierarchy with each step relying on the previous steps. Some claims may pay, deny, or internally pended in more than one of the six adjudication steps. For example, if the claim was submitted beyond the timely filing limit and the consumer is not eligible on the date of service the claim will deny in two of the six steps, consumer Eligibility and Provider Eligibility.

The following diagram illustrates the Six Steps of Adjudication within AMISYS. This diagram shows how the different subsystems are linked in hierarchy priority to process claims effectively.



A step-by-step description of the process follows:

Step 1 - Field/General Edits - The Field/General Edits step verifies that key information, diagnosis code(s), procedure code(s), modifiers, consumer number, provider number(s) are valid data types configured in the AMISYS system. Currently, AMISYS supports up to five diagnoses per service line.

Step 2 - Eligibility - The consumer Eligibility step verifies that the consumer, the consumer's Group and Division were eligible on the date the service was rendered. This step also determines if the consumer has other insurance coverage or if the consumer is on review or under investigation. In addition, the consumer's business segment and default configuration information specific to it is determined.

Step 3 - Provider Eligibility - The Provider Eligibility step verifies that the servicing provider, the referring provider, and the consumer's PMP were eligible at the time the service was rendered. It determines the providers' appropriate financial affiliations and if a provider is on review or under investigation. In this step, the system also determines if the claim is a duplicate service and verifies the claim was submitted within the allowed timeframe.

Step 4 – Authorization - The Authorization step determines if an authorization, pre-certification, or referral is required based upon the consumer's business segment, the providers' affiliations, the diagnosis, and the service rendered. If an authorization, pre-certification, or referral is required, the system will access the Authorization subsystem and search to find a corresponding record. If the system finds a match, the counter is decreased by the count on the service line of a claim.

Step 5 – Benefits - The Benefits step determines whether the service rendered qualifies as covered or not covered within the consumer's benefit package. Any applicable co-payments, or coinsurance amounts are calculated, and any applicable service limits, calendar year limits, or out-of-pocket maximums are counted. The system then determines if the limits or maximums have been met or are met with the current service.

Step 6 – Pricing - The Pricing step calculates the payment amount, if any, based upon the servicing provider's pricing configuration. For contracted providers, the pricing configuration will determine if the services on a claim are included in the capitated contract for a provider. The claim will be processed as an encounter claim if the service is in the capitated contract for the provider. If the service on the claim is not part of the capitated contract, then the service will be processed as a fee-for-service claim, accessing the fee schedule that is attached to the provider's pay class. Pricing for non-contracted providers is carried out in the same manner that Superior has configured for contracted providers. Non-participating providers are reimbursed according to the current Medicaid fee schedule, or by an agreed upon fee in keeping with ADHS/DBHS requirements.

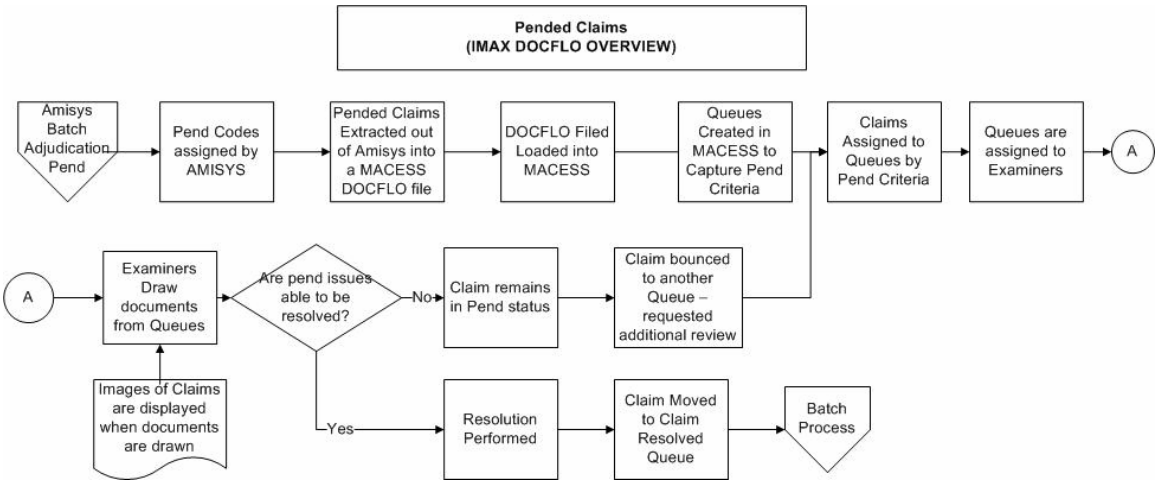
At any point during the above edits, Explanation (EX) codes can be returned to the claim to indicate whether the service is to be paid, pended internally, or denied. All EX codes are configured with text describing the circumstances for payment, denials, or reason for internal pends. These codes can be configured to appear on EOPs that are sent to providers to generate a separate letter (addressed to the servicing provider, the consumer, the referring provider, etc.) via the Correspondence Generator Subsystem, or to simply appear on internally pended claims reports.

If the claim fails any of the Six Steps of Adjudication, the system assigns the service line with an internal pend code.

3.3. Pended Claims Process

A Batch Claim Report is generated that reports the number of records in error that were not adjudicated and the reason for the error. It also reports the number of records passed, and the status of adjudication, whether the claims were paid, denied or internally pended. The records in error remain in the BATCH database and can be modified and corrected through the Batch Claims Processing entry screens. The records passed are written to the HEALTH database.

The following diagram illustrates the claim pend process:



If the claim passes all of the steps without being assigned an internal pend EX code, the claim will be sent through the Claims Payment Process.

3.4. Claims Payable Process

When a claim completes the adjudication process and results in a Claim Status of Payable, Denied, Denied-Additional Information, Rejected, or Denied-Duplicate, Centene issues checks for the payable claims if this service is contracted with the state. Checks are mailed to providers with the corresponding EOP as previously outlined in this document. Centene does not currently pay any provider via direct deposit, but can develop the 835 transaction to pay providers electronically as needed to meet ADHS/DBHS requirements. Centene does see the need and understands that this is the trend for future processing needs and thus will support the transaction fully.

4. Encounter Processing

Centene recognizes the importance of encounter processing and reporting and has dedicated personnel and hardware to ensure efficient, timely and integrated performance. As noted in other sections of this document in detail, the AMISYS system can collect, transmit and receive all of the data required related to consumer eligibility, providers, encounters, capitation and remittance. GREABHA also has the staff expertise to accomplish these requirements. GREABHA's systems can maintain consumer demographic and historical eligibility information and historical services provided with associated cost.

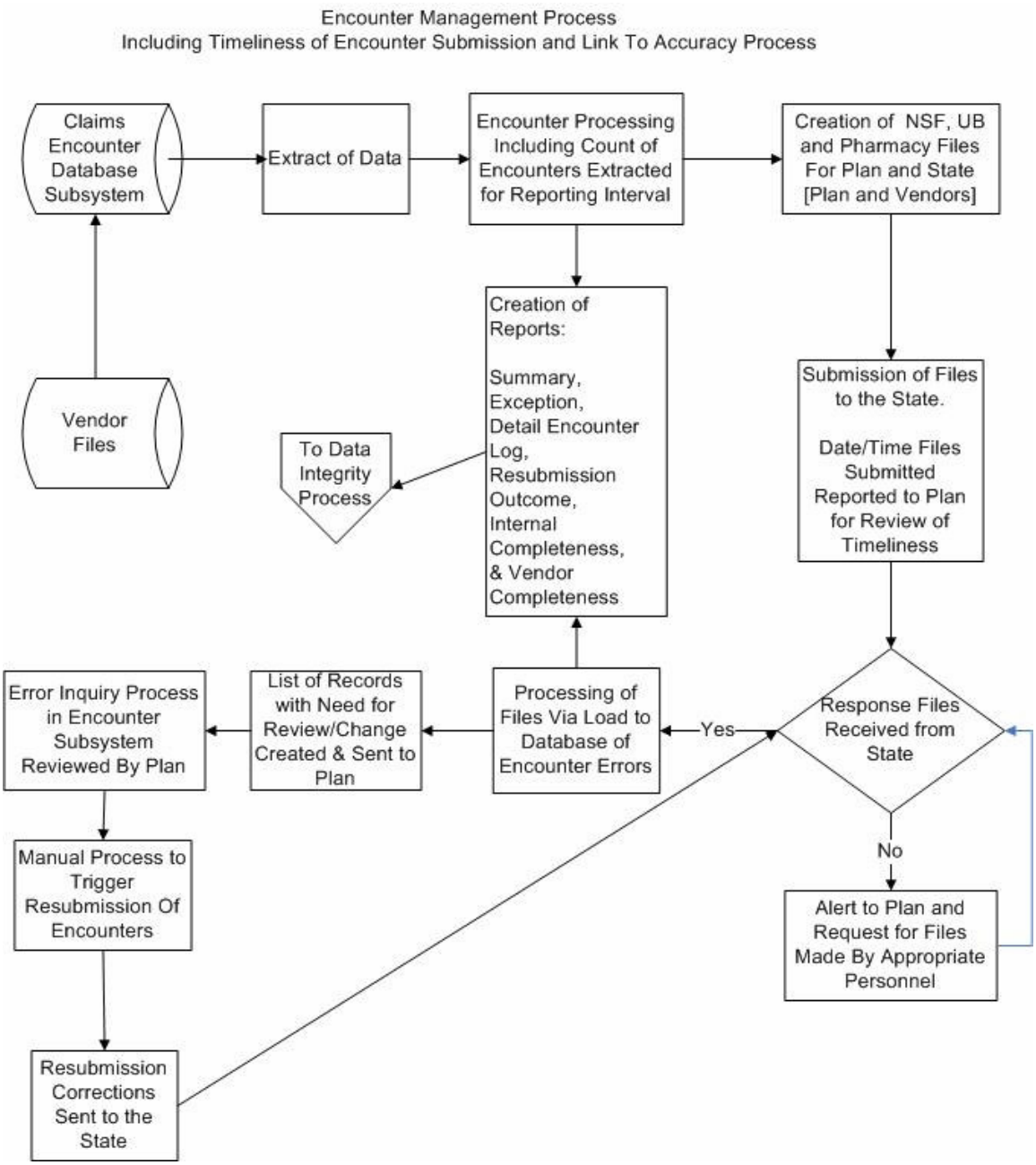
Centene's encounter reporting process makes use of the data produced via the claims submission process and validation steps through Centene-developed programs to build encounter files for submission. This process uses ADHS/DBHS standards to guide programming to include the needed data elements, needed file formatting and transmission mode.

The development of encounter files results in a series of reports to ensure data integrity, timeliness and completeness.

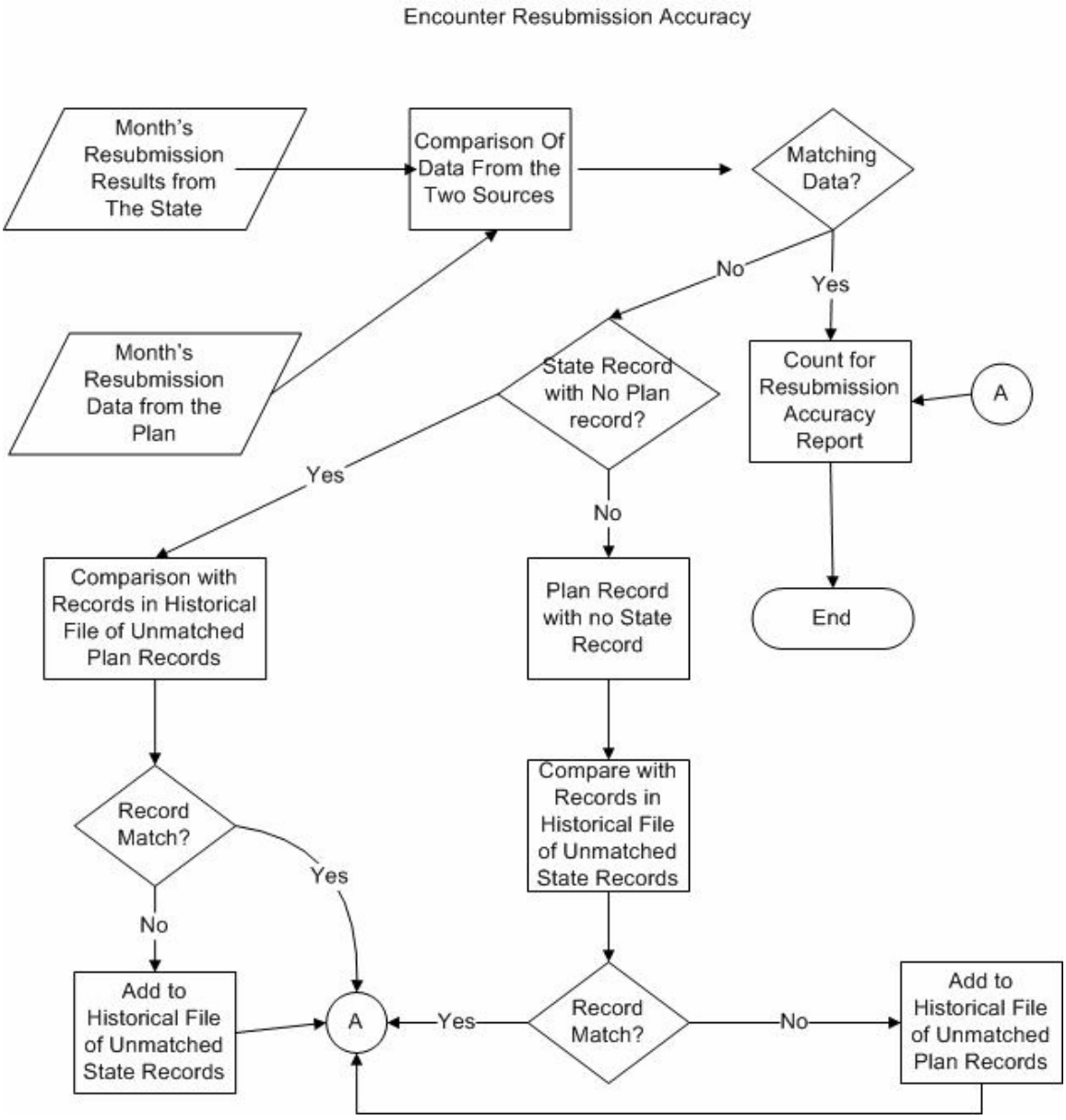
Encounter data is received monthly from our subcontractors. This data is stored in an external data set outside of our AMISYS processing system. Vendor data is batched and appended to the Physical Health data generated from AMISYS. Response reports are received by Centene's MIS Department. GREABHA can view these responses in an electronic format and then coordinate the responses based on the respective data issues. Vendors are then required to resubmit

corrected encounters. The reporting team and utilization management department conduct monitoring of vendor files, in conjunction with GREABHA Management. GREABHA holds their Vendors to strict requirements related to Claims and Utilization extracts.

The following diagram illustrates the Encounter Management Process:



The following diagram illustrates the Encounter resubmission process identified above:



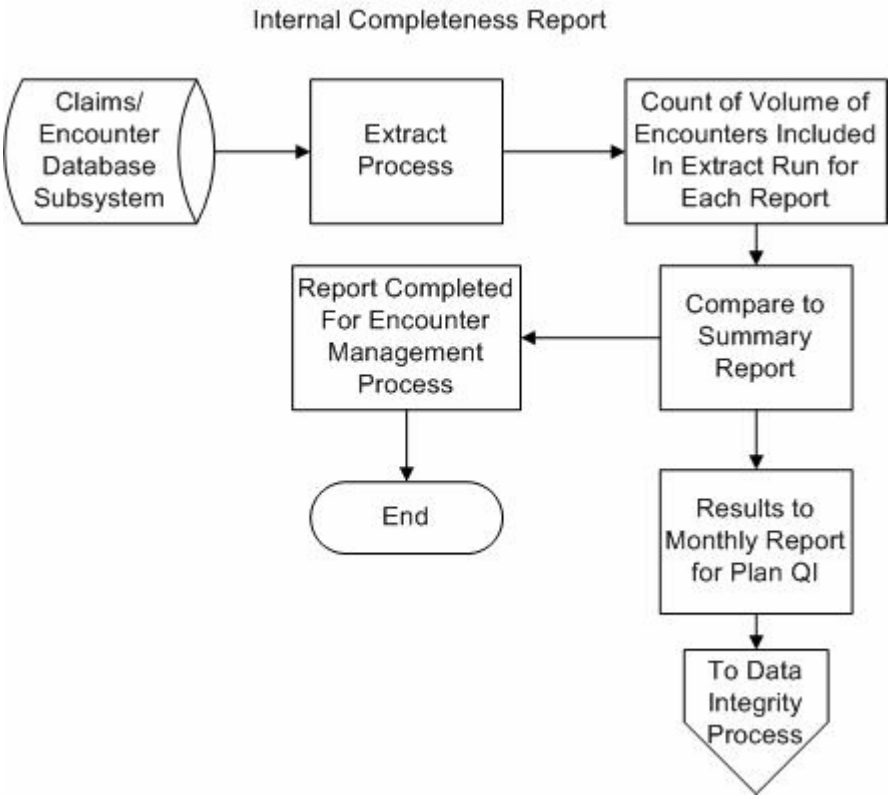
Centene's MIS Department will monitor performance of encounter submissions, including the formatting of data and file layout, based upon a review of standards and proposed submissions, performance feedback on files that have been submitted, and reports on performance in other areas [such as the timeliness of file submission against ADHS/DBHS standards]. These findings will be reviewed regularly with the MIS personnel dedicated to ADHS/DBHS business requirements and deliverables. Centene's MIS department has dedicated managers of both state reporting and claims liaison. Their focus is entirely upon deliverables, including the submission of all files, data and reports. Acceptance rates, for both submission and resubmissions, will be reviewed jointly by GREABHA and the MIS team.

Data validation can occur in stages, as agreed upon by ADHS/DBHS and Centene.

- Timeliness will be reviewed by GREABHA based upon routine reporting by MIS to GREABHA for each file submitted; email notices are automatically generated to GREABHA staff. As

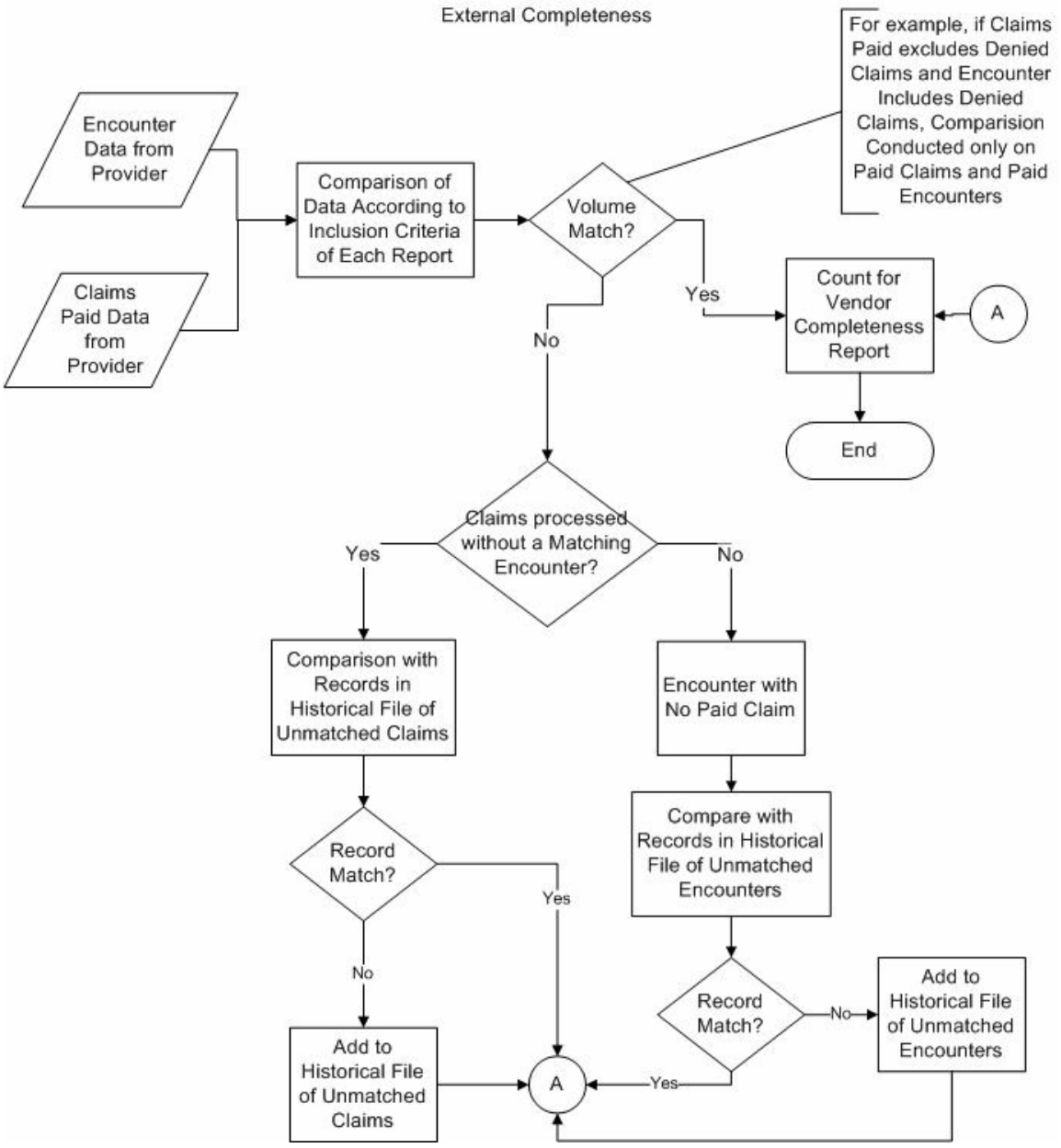
needed date and time of each submission can be reviewed. The MIS Operations Department logs each submission. Checks on job completion are conducted for each submission, and errors are rectified by on call programming staff or through the Change Request Process. If timeframes are not met GREABHA is contacted by MIS personnel.

- Change processes are also monitored by GREABHA and its MIS team. When a change is anticipated in the encounter submission or resubmission process, a formal process for the request for a new or changed MIS program and process is reviewed by GREABHA staff and MIS representatives, as judged needed by GREABHA. A formal request is submitted to a tracking software program that allows stakeholders to review progress on the request. Testing of the proposed change is conducted and GREABHA staff must approve the results of the testing. If acceptable, MIS then produces a schedule of the job for Operations, who execute the new program according to scheduling software. Completion of jobs is monitored and issues with production are managed by programming staff available at all times. This formal change request process ensures quality review and documentation of the changes being made. For this reason Encounter records are signed off at multiple levels for submission purposes.
- Completeness is monitored by GREABHA from internal and vendor completeness reports.
- The following diagram illustrates the Internal Completeness review process performed:



-

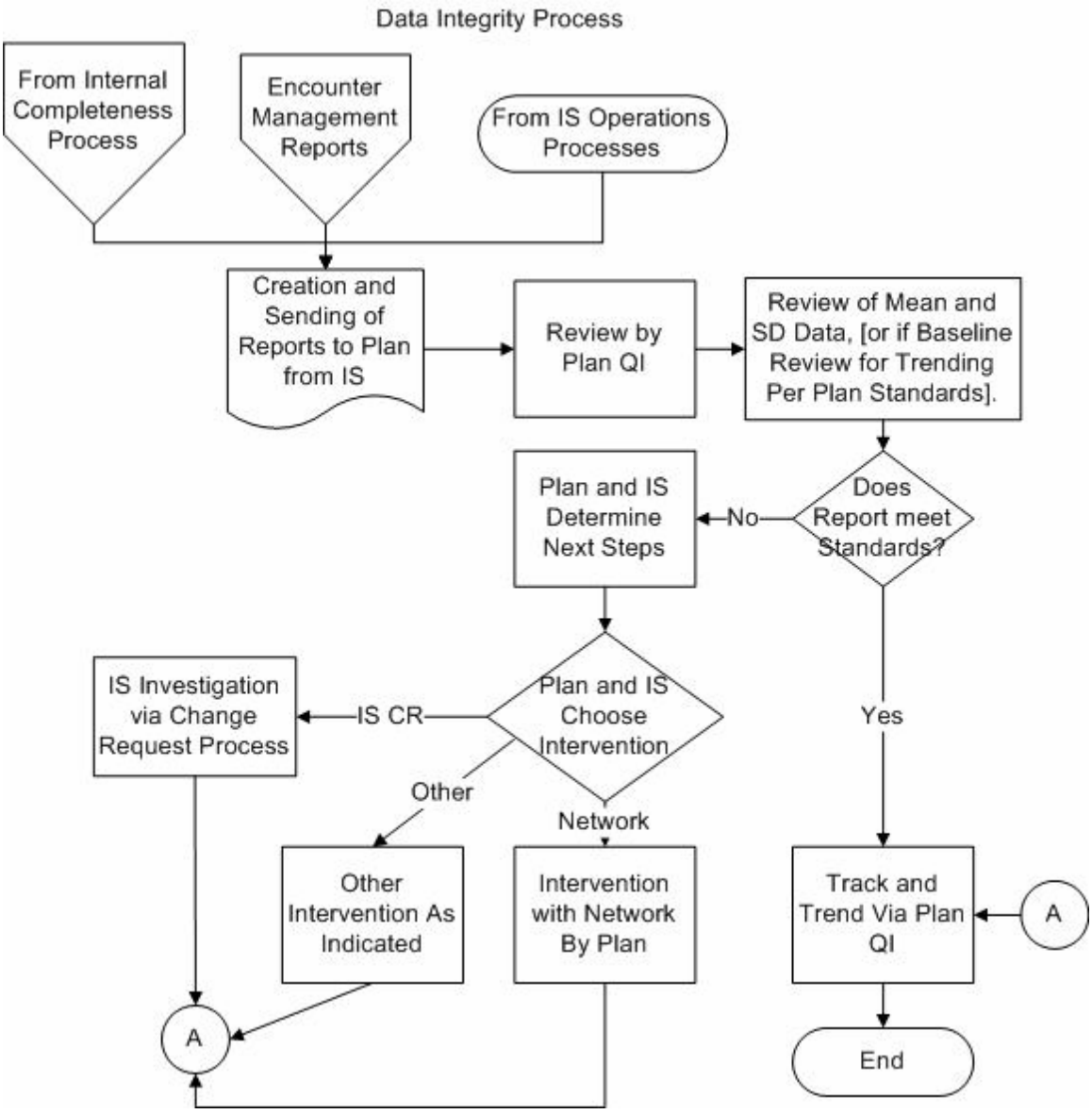
The following diagram illustrates the External Completeness review process performed:



- Exception Reports result from internal edit checks on claims data as it is transformed to encounter submissions. These reports will be reviewed by GREABHA regularly Exceptions do not stop an encounter from being submitted, but instead alert GREABHA to specific data quality items for the plan to monitor and address as needed.
- Detailed Encounter Logs of submitted files are maintained.
- Resubmission reports allow track and trending of the rate of encounters found to be in error by ADHS/DBHS, as well as the outcome of resubmission of encounters.
- Data integrity is monitored by GREABHA using the reports made available to them by MIS, including those noted here. Consumer benefits are clearly defined our system's Benefit subsystem and hierarchy. The Benefit Subsystem is part of the Six Steps of adjudication. These business rules are defined carefully through coordination with ADHS/DBHS by

Consumer Services, Provider Relations and Centene management as needed. The accuracy of applying these benefits to Claims payment are then ensured and thus encounter reporting in HIPAA compliant transactions is accurate and appropriate for analytical decision making.

The following diagram illustrates the Data Integrity Process performed to ensure the encounter management process is designed and maintained in accordance with program standards:



5. Utilization Management

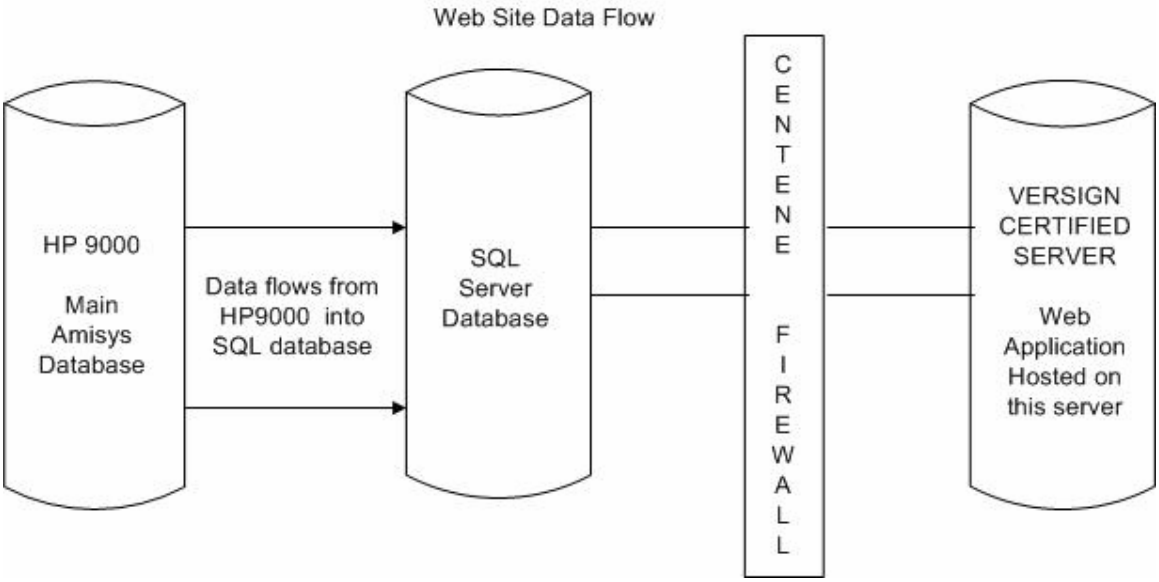
As mentioned previously, Centene uses McKesson's CareEnhance Clinical Management Software (CCMS) to automate workflows and clinical decision support criteria related to utilization management and case management. The Data Flow Overview diagram illustrates the CCMS interfaces for both inbound and outbound processes with AMISYS. The inbound data interface supplies updated provider and membership information for the care coordination staff. This update occurs on a daily basis and is an automated process. The outbound interface from CCMS to AMISYS updates the claims system with authorization records for higher levels of care. These records are mapped and loaded into the Authorization dataset for adjudication purposes.

Centene also utilizes CareEnhance Resource Management (CRMS), a McKesson suite of customizable analytic tools, to allow monitoring, profiling and reporting on the treatment of specific episodes, care quality and care delivery patterns. CRMS enables us to identify our cost drivers, to help guide best practices, and to manage variances. As seen in the Data Flow Overview diagram, CRMS is updated on a monthly basis by using an interface that extracts claims, consumer, provider and financial data. This is data is then transmitted to McKesson. McKesson then maps this data to their tool, CRMS, which is then made available for the Utilization Staff to run standard queries or create ad hoc queries on the fly.

6. Web Site Data Flow

Centene's capabilities include being able to support the appropriate flow of data from the core system to a secured Web site. Because the core data resides within AMISYS, extracts are generated daily which populate a SQL Server database. This data is then mapped to the Web Server for updating to the Internet.

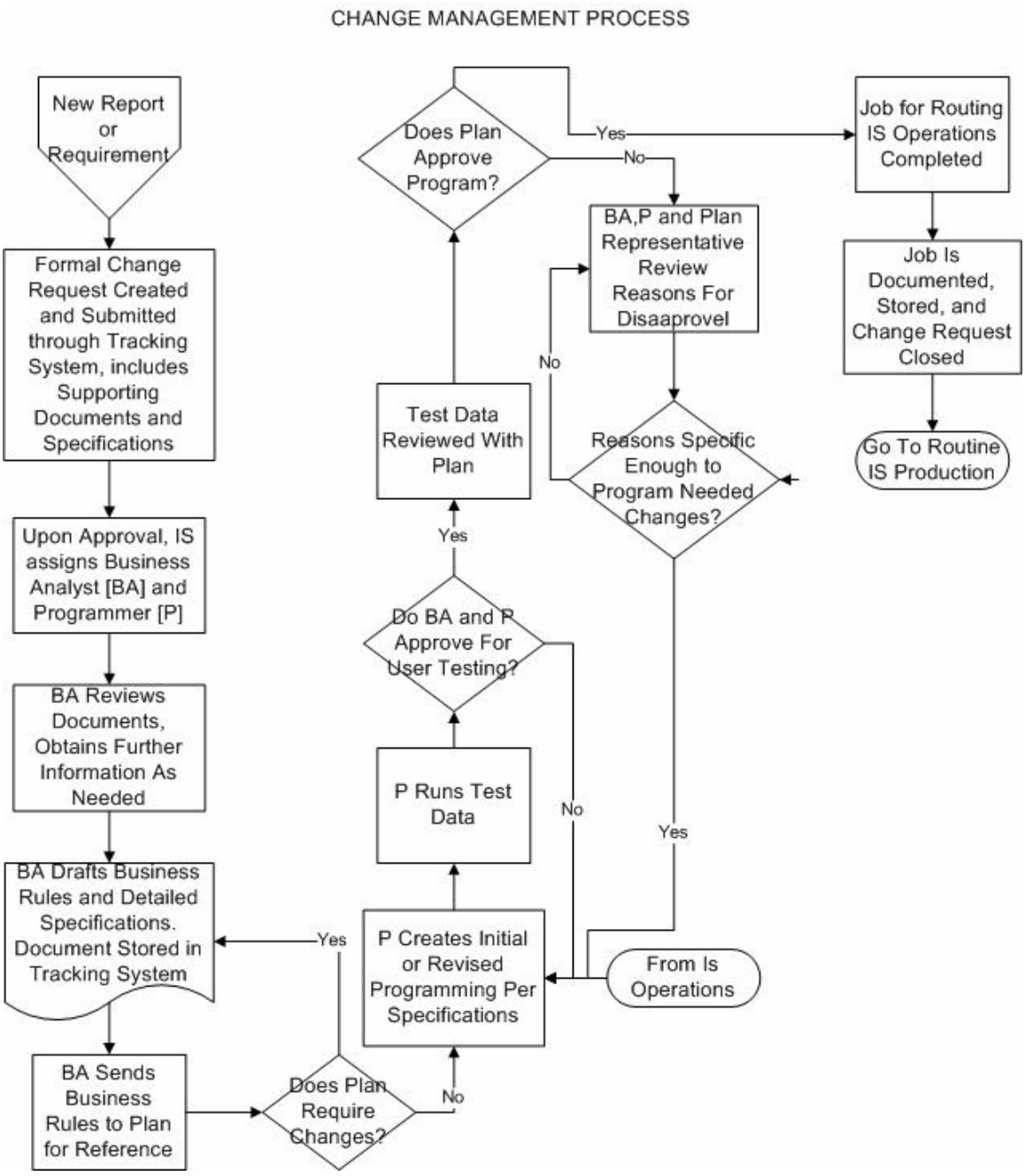
The following diagram illustrates Centene's web site data flow capability:



7. Change Management Processes

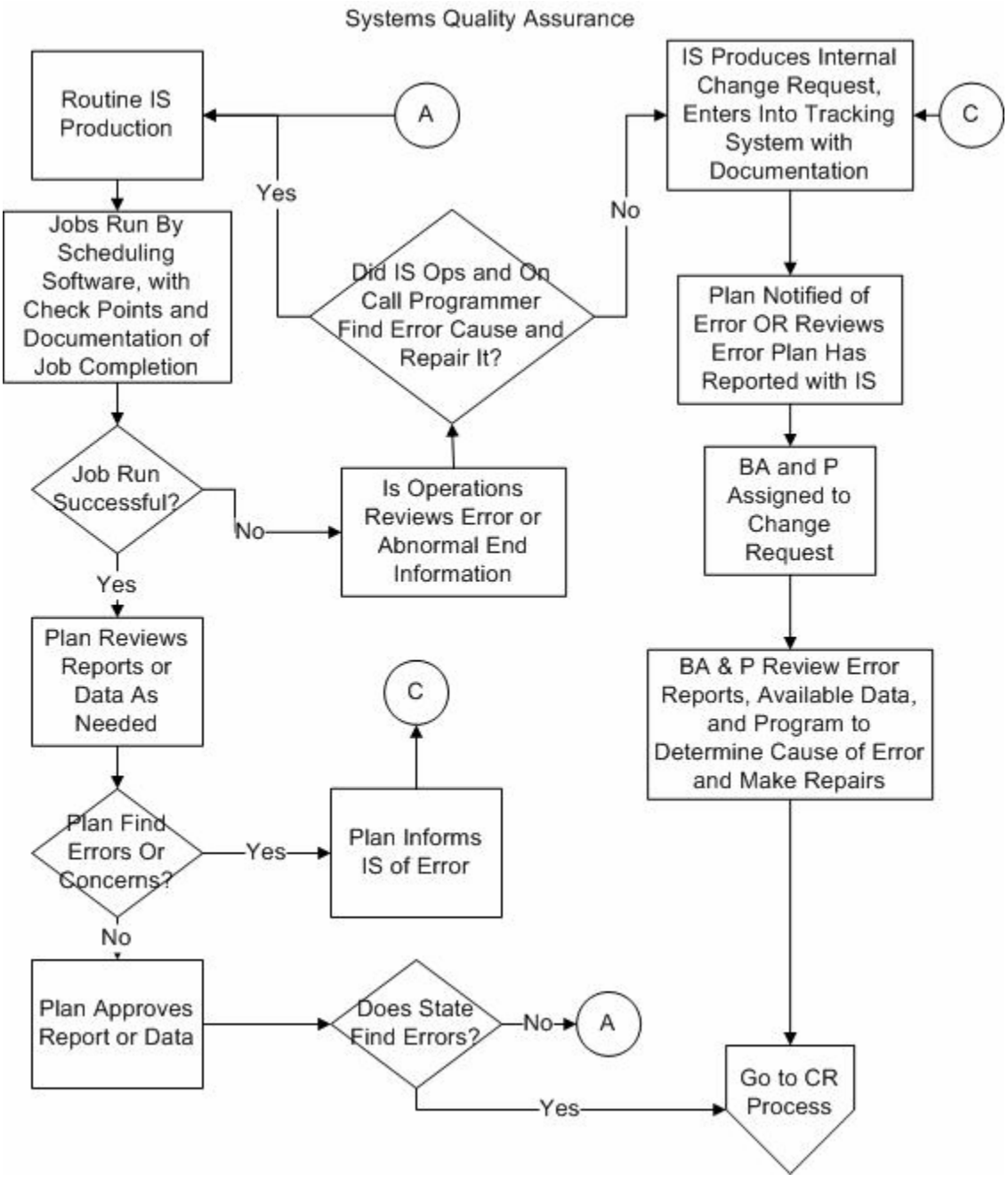
As outlined in various previous sections, Centene utilizes a change control process to implement system changes that are needed as a result of system upgrades, error resolution, or process improvement.

1 The following diagram provides a visual flow of the change request process:



2

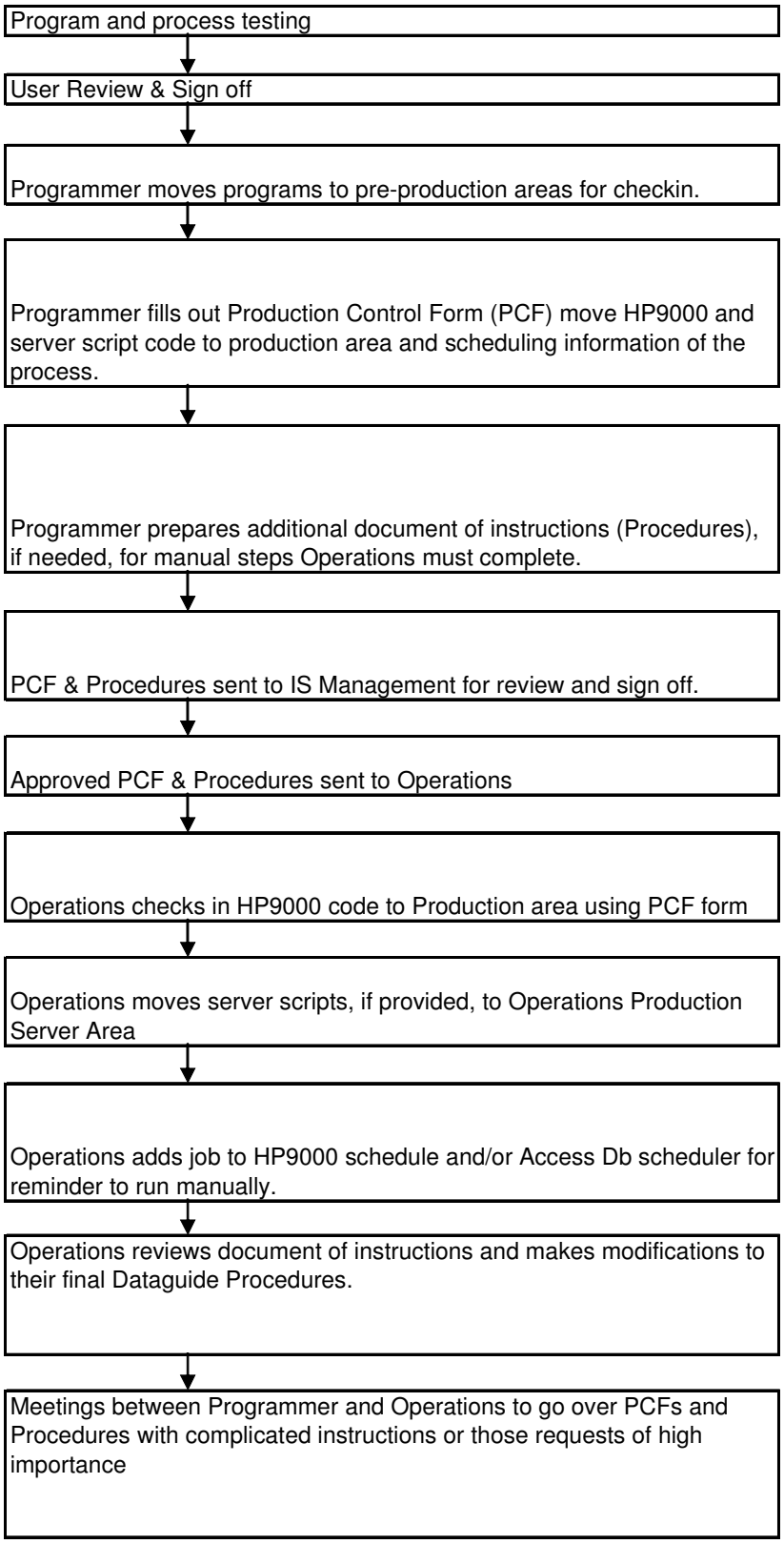
Step 10 above indicates the monitoring of jobs, which is illustrated in the following diagram:



8. IS Operations – Internal Processes

Centene's Operation's staff employs both manual and automated processes. All procedures are cataloged online in a Dataguide, which automatically updates as changes are made. The Dataguide is detailed procedural guide that explains both manual and automated processes related to running programs and notifying Operational staff accordingly. The Operation's staff utilize an Access database to track all daily, weekly, monthly, and yearly processes that facilitate eligibility, remittance and deliverables functions in an efficient, timely manner to ensure that due dates are met. The Operations staff also has automated Scripts that pick up files from the BBS system and/or Vendor's FTP sites that place them on the HP9000 or network drives for processing.

The following diagram illustrates the process to update programs and the Operational procedures to ensure that the Data Guide stays updated:



9. Coordination Of Benefits and Third Party Recovery

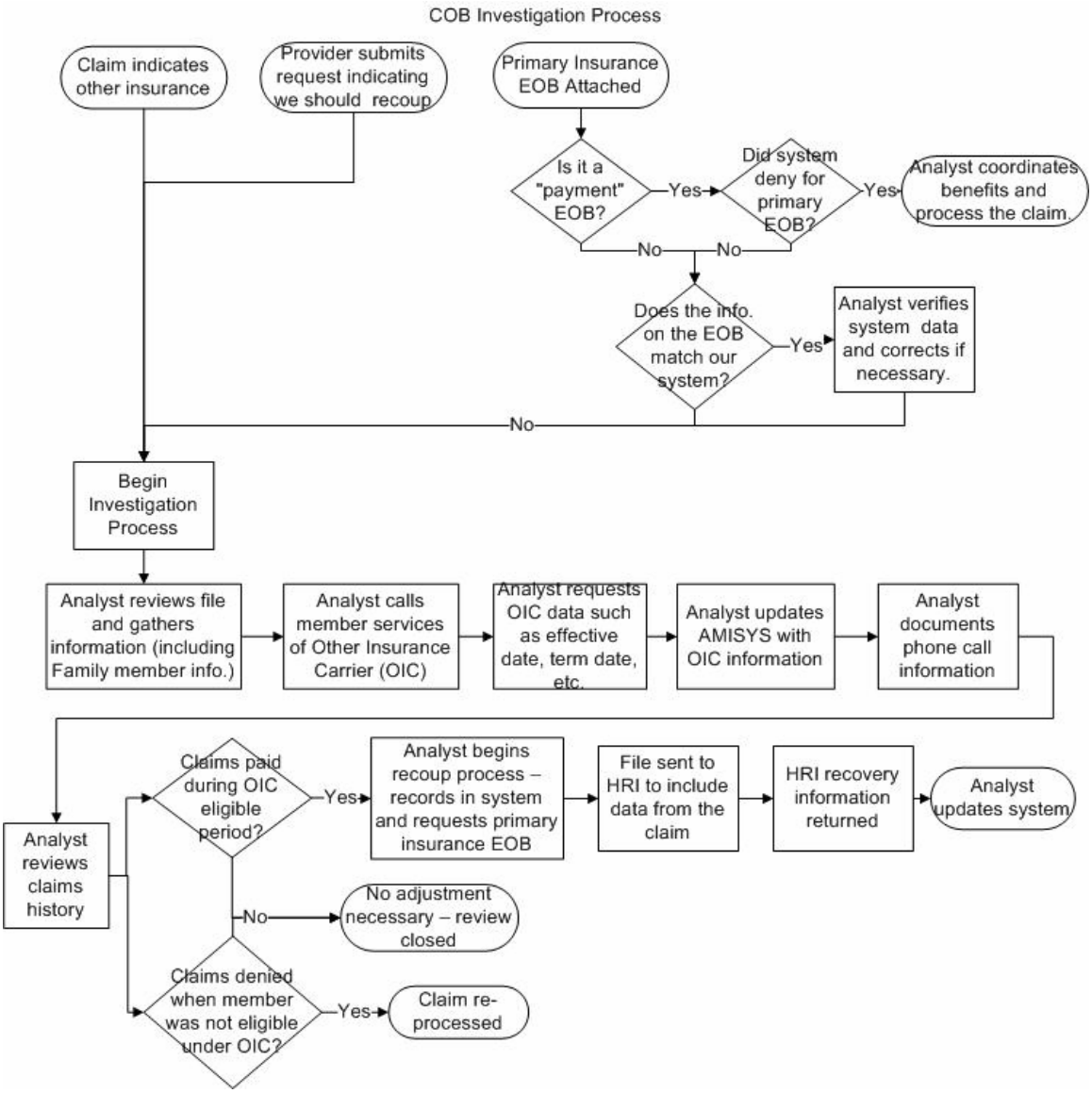
9.1. Process

The COB Department, trained on the state-based Coordination of Benefits (COB) regulations, identifies and pays/denies claims based on Members having two or more types of insurance coverage. They are responsible for:

- identifying the Members primary insurance
- ensuring that the primary carrier pays its full benefits first
- keeping up to date with Consumer's other coverage through ongoing investigative work

The COB department coordinates payment by using ADHS/DBHS's requirements for determining primary's payment and primary's allowable. Primary payment is the payment made by primary including any discounted amount. Primary allowable is the total amount paid including discounted amount plus total consumer liability.

The following diagram illustrates the triggers and process for coordinating and investigating potential COB savings:



9.2. Reporting

There are two reports that track COB savings per month, quarter and year:

- COB savings report – represents dollars saved by processing charges as secondary payer versus primary payer.
- COB cost avoidance report – represents dollars saved by both manual recoupment/denials and systematic denials of claims not submitted with primary carriers EOB

9.3. Third Party Recovery

CBH works with HealthCare Recoveries (HRI) to handle claim submissions related to subrogation. Every month a file is sent to HRI, which includes information regarding all claims processed for CBH the previous month. HRI reviews the tape and identifies those claims that have potential possible subrogation involved. Once that determination is made HRI begins the process of chasing and recovering. Each month HRI sends a report to the COB department showing those claims that were recovered for the prior month. The COB department then updates the claims system with the appropriate information.

I. Testing Plan and Data Conversion

1. Overview

Centene contributes a proven model for transitioning and implementing Medicaid services business in various states, providing the structure and organization necessary to effectively execute all required implementation and readiness activities and meet the most aggressive of timeframes. Centene is committed to maintaining high performance levels and effective communication channels well beyond the Transition Phase of a contract implementation. This transition involves all functional areas of the organization, including the IS department and its responsibilities related to the transition. We have therefore explained our general implementation approach and the specific IS Planning and Implementation approach to illustrate our commitment to this process.

Centene's testing plan and data conversion approach places a high priority on preventing any adverse impact on program stakeholders (ADHS/DBHS, consumers and providers) from the transfer of responsibility to Centene. In addition to its time-tested Transition Implementation Plan approach, Centene manages a Key Issues contingency planning tool that enables Centene to track and resolve issues identified during the Readiness Review process. Once all identified Key Issues are resolved, Centene's Performance Improvement Team (PIT) approach continues to refine work processes resulting in maximum measurable benefit for Centene customers and program stakeholders. The PIT has proven to be especially useful in ensuring that a seamless transition continues into a problem-free operation.

Through the narrative response and tables provided below, Centene will illustrate how it will conduct all implementation and transition activities related to the implementation of the ADHS/DBHS business product, as well as post-transition support and long-term operational cooperation. Given Centene's experience and track record with implementations and transitions, ADHS/DBHS can be assured of an efficient, cost-effective transition outcome with limited impact on stakeholders.

In a transition situation, Centene develops an over-arching Transition Plan, which clearly communicates the Transition Project Objective, the Project Team, Project Timelines and the Transition Matrix. The Transition Matrix, included as a table herein, is a key working document in this package. The Matrix identifies every action that must occur in order to successfully transfer operations from the current vendor to Centene within the established timelines. Centene manages the project, in conjunction with ADHS/DBHS and the current vendor(s) as applicable, through consistent communication and reporting. This process in described in greater detail below.

All systems and operational structures, business operations, policies, procedures, work processes and tools discussed in this section are Confidential and Proprietary to Centene, Centene Corporation and its affiliates. This information should not be shared with any entity outside of ADHS/DBHS without specific consent from Centene.

2. Overall Project Management Approach

Centene has found that a highly-effective Transition Project Team approach is critical to the success of an implementation of this magnitude. Centene's Transition Plan and the process described below will demonstrate the level of integration and communication necessary to effectively manage the project. The Centene Transition Plan is an over-arching document which clearly defines the Transition Project objective(s), identifies the Centene Transition Project Team and key project issues, and includes the Transition Matrix. The key "working document" central to

this process is the Transition Matrix. The tools used to manage implementation projects are designed to be flexible and are customized to fit the requirements and elements of the different processes.

The Transition Matrix addresses the following functional aspects of a Transition situation:

- Organizational aspects of the project (contact lists, workgroups)
- Regulatory requirements, such as licensure and contract execution
- Financial reporting
- Transfer of data: eligibility, inpatient status
- Consumer specific records and documentation for case management
- Stakeholder communications
- Information Systems
- Interfaces with ADBH/DBHS delegates
- Benefit configuration
- Back-up and disaster recovery plan
- Reporting, including encounter data
- System testing
- System readiness assessment
- Operational Readiness Assessment
- Consumer and provider communications & materials
- Network development and Credentialing
- Staffing and training
- Infrastructure functions (telephones, workstations, office space)
- Policy and procedure development and review
- Case Management Transition
- Scope of benefits and Value-Added Services
- Claims cross-over process
- Claims run-out procedures
- Continuation of reporting, record retention
- Any additional elements as required by ADHS/DBHS

The following sections describe key processes performed as part of the transition phase.

2.1. Establish Project Objectives

At the initiation of the contract, Centene, ADHS/DBHS and other parties, as required, will participate in an initial meeting in which ADHS/DBHS identifies the desired outcome(s) for the project, the requirements for achieving the outcome(s) and the timeline under which the project will be completed. This meeting will provide the framework within which Centene personnel and all other parties will operate. Transition Project documentation will then be developed to fit the parameters set forth by ADHS/DBHS, understanding that changing circumstances can change the direction, complexity or timing of the project. During this meeting, the project teams and key contacts responsible to ADHS/DBHS for the duration of the project are identified.

2.2. Transition Plan and Matrix

Once ADHS/DBHS provides direction to Centene and other parties, Centene's Transition Plan document and Matrix will be developed and customized to reflect the specific issues related to the project. Centene's draft Transition Plan and Matrix will then submitted to ADHS/DBHS for review and approval. Any changes to the Plan or Matrix, requested by ADHS/DBHS, are then incorporated into the respective documents and submitted to ADHS/DBHS for final approval.

Centene's Transition Matrix is central to the successful management of a transition situation, as it clearly outlines all components of the Transition process, including the proposed schedule,

activities and resource requirements, that must be followed by all parties to meet both Centene 's and ADHS/DBHS's expectations. The Matrix is organized according to the entity that has primary responsibility for completing the element, while cross-referencing all parties involved in the implementation of each element.

Centene utilizes the Transition Plan and Matrix as its internal project management tools. All items included in the Plan are assigned to a member of the Centene Transition Team for execution and reporting. Centene conducts an initial Project Team meeting in which the CEO and Transition Team Lead present the scope and objective of the project and walk through the elements of the Transition Plan. This meeting serves to emphasize the priority status of the project and to ensure comprehension of the tasks at hand. It also facilitates discussion and raises issues or areas of concern to the appropriate level for problem resolution. In some cases, issues are taken ADHS/DBHS's Transition Project Team meeting. All issues and resolutions are communicated back through Centene's Transition Project Team Lead to Centene personnel responsible for implementing the Transition Plan.

2.3. Ongoing Communication with ADHS/DBHS

Throughout the Transition process, Centene communicates with ADHS/DBHS and other involved parties through weekly status meetings conducted by ADHS/DBHS. These meetings allow ADHS/DBHS to fully review the status of all parties' activities, address any concerns related to performance or timeliness, and to understand any operational issues that may have been identified during the previous week. Any substantive issues that could potentially threaten the performance of Centene or ADHS/DBHS are reported to the designated ADHS/DBHS representative immediately through the Centene Project Team lead. Centene's Transition Project Team lead helps to facilitate constant communication with all parties so that the overall project objectives can be achieved.

2.4. Risk Management Plan

Centene's approach to risk management is integrated into its Disaster Recovery and Business Continuity process. A Disaster Recovery and Business Continuity Plan will be established to specifically include the systems and process to support ADHS/DBHS.

2.5. Post-Transition Deliverables

During the final meeting of the ADHS/DBHS Transition Project Team, the plan for post-Transition services and deliverables is finalized. Requirements for continued reporting are communicated to the appropriate parties and deliverable timelines are defined. Centene makes all final adjustments to its Transition Matrix pursuant to this final meeting, and any required deliverables are submitted by Centene to ADHS/DBHS in whatever format or schedule is required by ADHS/DBHS.

Centene understands that ADHS/DBHS may, at any time, request additional information beyond that which was originally approved, or as modified by ADHS/DBHS. Centene is willing to balance changing priorities and timelines, within reason, to meet the needs of ADBH/DBHS, consumers and providers and to successfully accomplish a seamless transition.

3. Systems Development and Implementation Project Plan

A key element in the Transition Plan is the Systems section, which the IS group develops in further detail. The implementation project plan accounts for full system builds and testing processes that include all appropriate operational departments. The project plan details both State deliverables/interfaces and the assessment and configuration tasks needed to meet milestones. Also used in any transition or implementation project is the Information Systems

business assessment tool. This tool is the basis for our initial business evaluation. Operational and MIS business rules are generated from this tool and applied to the implementation workflow.

Centene systems are adaptable to changes in Business Practices and Policies in the timelines identified in the RFP. Any major systems changes initiated by Centene will be reported to the ADHS/DBHS staff contact 90 days prior to implementation of the system change. In the case that a Centene system change would impact the operational business processes that occur between Centene and the State of Arizona or the State's administrative agents, a complete change over plan would be submitted at the 90 day timeline. The plan would include the system changes, their impact on business processes including any output changes and a cost benefit analysis if applicable. The plan would be inclusive of an implementation schedule and key contact person to which the State could address questions or concerns.

Centene believes that establishing an avenue for continual communication flow is critical to the success of product administration. Centene will establish an official point of contact with ADHS/DBHS staff on an on-going basis including Internet E-mail address, work day telephone numbers as well as after hours and holiday contact information for emergent situations.

Following is the content of a sample Project Plan used by the IS Implementation Team in managing the information systems development and implementation:

I CENTENE IMPLEMENTATION COMMAND & CONTROL
Establish Weekly Review Meetings
Complete Scope Document
- Draft Scope Document
- Submit/review 1st draft
- Submit 2nd Draft to Director for review
- Submit Final Scope Document to Director for approval

ICR Rollout
Document State Contact List
Complete Security Level Template
Rollout Spec Templates
Secure Resources
- MIS Internal
- MIS External / Contracting
- Plan Participants
- Operations

II READINESS REVIEW: Interface Testing for Certification
Create test files for encounter data and test with the state
Create test files for appeals and test with the state
Create test files for grievances and test with the state
Create test files for SACMS and test with the state
Create test files for PCP files and test with the state
Test relationship of interfaces with other subsystems
- Encounter interface
- Appeals/Grievances interface
- Other interfaces

III ESTABLISH BASELINE SYSTEM
Install State Amisys Tape
Benefits Functions
- Benefits Grid
- Create Benefits Spec

Encounter Functions
- Process
- EDI
- Create Spec

Eligibility Functions
Batch Load Process

- Real-Time Processing
- Reconciliation
- Create Eligibility Spec

Finance Functions
- Claims Payable
- 1099
- Funding
- G/L
- Create Finance Spec

Utilization Management Functions
- CCMS Configuration Analysis
- Create Spec

Operations / IT Functions
- Batch Jobs
- Schedules
- Procedures
- Create Operations / IT Functions Spec

Phone Log Functions
- Setup
- Create Phone Log Spec

Pricing Functions
- Contracts
- Fee Schedules
- Code Set / Keyword Structures
- Create Pricing Spec

Provider Functions
- System Maintenance
- Create Provider Spec

Reference & Controls Functions
- Business Segment Structure
- Code Sets
- Super Table Entries

Reporting/Interface(s) Functions
- Standard Reports
- Custom Reports
- State Reports
- Vendor Xfaces
- Create Vendor Interfaces Spec
- Create State Reporting Spec
- Create Reporting Spec

Security Functions
- Complete SecLevel Document

IV HARDWARE/OPERATIONAL SETUP

ESTABLISH State BASELINE ENVIRONMENT
- Create Baseline Account from State

ESTABLISH State DEVELOPMENT ENVIRONMENT
- Eliminate Non-Standard Configs. / Data

ESTABLISH State PRODUCTION ENVIRONMENT
- Create Production Accounts
- Establish / Implement Change Control Procedures

V SYSTEM SETUP & CONVERSION

Includes configuration of each of the above listed functions under establish baseline system

Includes identification of training needs in each above listed functional area

VI NEW SYSTEMS IMPLEMENTATIONS / CENTENE STANDARDS

Centene Claims Standard Operating Procedures (S.O.Ps)
- Paper Claims
- MACESS

- Planning Meeting
- Complete Scope Document
- Copy Vertex Templates and attributes
- Quality Assurance
- I/S Testing
- Programming - Internal
- Migration of change to Test Account
- Load of files
- User Acceptance Testing
- Sign-off
- Plan End User Training
- Claims User Training
- Migration to Production - Go Live
- Post Implementation Cleanup/Issue Resolution

Coordination of Claims
Identify Training Needs

Centene Provider S.O.P.s
Data Validation / Cleanup
Identify Training Needs

Centene Med. Mgmt. S.O.P.s
- Code Review
- Create Code Review Specs
- Setup / Implement Code Review
- Identify Training Needs
- Determine CRMS Need (Assessment)

VII SYSTEM TESTING

Includes unit testing for each of the above listed functions under establish baseline system
Includes testing of process functions

VIII IMPLEMENTATION ROLLOUT

Create Implementation Rollout Spec
Create Rollout Schedule
Create On-Call / Backup / Support - Escalation Plan
Execute Go-Live

The Sections below describe key processes performed under this IS Implementation Project Plan:

3.1. Business Requirements Gathering/Assessment Tool

Any program implementation is only as good as the quality of the business requirements used to develop the systems. Therefore, Centene approaches each MIS implementation project by performing a requirements gathering process for each functional area and documenting these specifications.

Following is a sample specifications document which outlines the information produced during this process to ensure that appropriate and thorough requirements are captured:

Introduction	This section should describe the purpose and scope of the functional area being converted / implemented; a brief system/project background description, and references used to develop the mini spec

Purpose	Describe the purpose of the conversion mini spec. The mini spec should clearly define the system or project's conversion procedures; outline the installation of new and converted files/databases; coordinate the development of file-conversion programming, and mini spec the implementation of conversion procedures. Depending on the factors that must be considered for each functional area, the conversion mini spec should consider the following: • Determine if any portion of the conversion process should be performed manually • Determine whether parallel runs of the old and new systems will be necessary during the conversion process • Understand the function of the data in the old system and determining if the use will be the same or different in the new system • The order that data is processed in the two systems • Volume considerations, such as the size of the database and the amount of data to be converted; the number of reads and the time required for conversions • User work and delivery schedules; time frames for reports, etc. • Whether data availability and use should be limited during the conversion process • The disposition of obsolete or unused data that is not converted
Scope	Provide a general description of the boundaries of the data conversion effort. This may include the specific system functions affected; functions/data not affected/converted; discussion as to whether the conversion process will be implemented in phases or stages; what data related to certain business processes will be converted first, etc. *Note: Multiple conversion mini specs may be required if a system is to replace several different current systems*.
Conversion Requirements	This section should identify the data to be converted (input); the process by which the conversion will be done; the conversion results (output); and the method used to validate the conversion
Input Data	Provide a description of the data that must be converted (prior to its use in the proposed system). The description should include its name, source form or record layout, storage medium, location, volume, size, access method, and any security considerations.
Specifications	Describe in detail how the conversion will be accomplished. If computer programs are to be used, provide their specifications, e.g., program logic, interfaces, error/exception processes, etc.
Output Data	Provide a detailed description of the data that will result from the conversion process. The description should include its name, record layout, storage medium, location, volume, size, access method, and any security considerations.
Output Data	Provide a detailed description of the data that will result from the conversion process. The description should include its name, record layout, storage medium, location, volume, size, access method, and any security considerations.

Programs Affected	Identify the programs affected as a result of the conversion of data. Provide a listing containing the program, and the nature of the change.
Validation	Provide a detailed description of the manual and/or automated controls and methods to be used to ensure that all data intended for conversion has been converted and that all programs affected are operating correctly.

3.2. Interface Requirements

Centene currently operates a HIPAA-compliant information system that is configured to consistently accept and transmit information. Centene will coordinate with ADHS/DBHS during the transition phase of project implementation to ensure appropriate transmission processes and functions are built to support ADHS/DBHS requirements. In addition, Centene will acquire the necessary hardware and as well as build the necessary telecommunications infrastructure to facilitate the ADHS/DBHS program as contracted. Because we currently perform similar services in other states, this structure's design has been tested and proven. Centene's information and communications systems will consistently support operational performance to meets or exceeds the standards set forth by ADHS/DBHS. Any modifications to these systems required to support business functions of the new contracts will be planned, installed and tested in accordance with the approved transition project plan.

Technology allows Centene to use BBS, FTP and Web portals to quickly receive, process and send data in a manner that meets its high standards for data quality and integrity. This, in turn, benefits Centene personnel who can more effectively meet Consumer's needs and respond to providers' questions. Centene information submissions will be designed to meet ADHS/DBHS's directives for format and timeliness.

3.3. Joint Interface Plan

Centene has developed a number of Joint Interface Plans (JIP) in order to communicate and coordinate the development and testing of file formats. Systematic tools are used to track and schedule these processes so that manual intervention is limited. This method of building and creating procedures that are clearly communicated minimize the costs related to maintaining these programs.

3.4. Information Transfer

Centene's Information Systems Implementation and Integration Team will be deployed to perform the tasks necessary to implement the program. The Implementation Team and IS personnel are experienced in both start-up and acquisition and with systems and transition integration. A Centene Information Systems Director will oversee any transition project undertaken by Centene. Transition of claims data is a focal point in each transition. Centene's scope and project planning documentation details both paper and EDI transitioning. Centene's Transition Plan and Matrix address all transfer requirements in detail, down to the specific element. Each information transfer element is specific to the type of information to be reported, the data elements required to complete the transfer, the individual(s) to whom the report should be submitted and the timeline. In cases where the same data is to be provided on separate occasions, i.e. case management components, direct links of communication are established between the parties to allow for efficient data transfer so that care coordination efforts are not disrupted.

Centene constructs its Transition Matrix to comply with the data transfer requests and timelines of ADHS/DBHS, and plans all action items in order to meet such directives. Additionally, to further

detail the intricacies of Information Systems migration, the Director develops an MIS specific project plan to ensure the team's success.

3.5. System Readiness

All transaction processing is tested thoroughly by Centene's MIS department, the effected Department and Quality Assurance. Testing is documented and kept for historical reference and trouble-shooting.

In order to demonstrate systems capabilities and readiness to administer the ADHS/DBHS product, Centene will conduct extensive testing according to an ADHS/DBHS provided test plan and as provided for in its state approved MIS Project Plan, Joint interface Plan and overall Transition Matrix.

In addition, Centene will secure an Independent Verification and Validation certification of the following items:

- Facility security including all appropriate building inspections and fire and safety approval
- Facility hardware and software applications are HIPAA compliant and secure
- Facility Management Information System (MIS) has the capacity to administer ADBH/DBHS business

All testing and independent verification activities will be completed and reported to ADHS/DBHS prior to implementation and are subject to ADHS/DBHS approval.

System readiness will be further verified through Centene's participation with the State in onsite and desk reviews assessing systems readiness. Centene understands that interface and application flow charts must be delivered to ADHS/DBHS 60 days prior to readiness testing and that system readiness and facility review will occur 30 prior to implementation.

3.6. Testing

Both Unit testing and end-to-end testing are performed across the various functional areas of the organization. Testing objectives include to validate and review that all configuration, pricing, encounter processing, authorization, provider, eligibility/benefit, and EDI modifications, etc. produce the expected output data. This includes testing the internal programming and configuration set-up as well as the Product Change Requests (PCR's) or modifications made by AMISYS Synertech.

Each tester within the IS department and functional area representatives are assigned specific responsibilities to perform as part of the testing process. These include:

- Testing PCRs applicable to functional area.
- Testing all daily activities/critical functions, including any non-routine scenarios.
- Recording and reporting testing results to the designated MIS Contact.
- Working with other teams for system testing. For example: The Claims Team may have a scenario that requires assistance from the Provider Network Team. Or the Utilization Management Team may need the Membership Team to create/modify Consumer data for a certain scenario. We must all be willing to work together to complete the testing process.
- User Acceptance Testing Form - This should be completed for each PCR tested/reviewed (pass, fail, or n/a). After all PCR's have been reviewed, "daily activities" testing is performed to ensure all the screens that are used on a daily basis are functioning as usual and

performing as expected. A User Acceptance Testing Form will need to be completed representing "daily activities testing".

- If any Run-Screens or custom screens must be tested as well, along with a form completed to include the test results.
- Jobs or programs related to job functions within a functional area are tested and a form submitted with the test results.
- User Team Sub-System Sign-off - This should be completed once all testing of the PCR's in the functional area are complete.

Each tester logs and tracks the following results during the testing process:

- Test Case ID
- Screen
- Version
- Record
- Number
- Test Case Description/Objective
- Expected Results
- Actual Results
- Pass/Fail/Incomplete (P/F/I)
- Test Date
- Status/Comments
- Tester

During testing, issues must be reported to ensure the issue is de-bugged properly. These steps include:

1. All issues must be documented in issue area of User Acceptance log with a description of the issue/bug and forward to the QA coordinator (review coordination grid) when completed. If there is a modification/change that can correct issue/bug, the modification/change must be listed in detail in the modification field (if tester can make the changes). **No modifications/changes can occur without notifying QA.** If tester cannot make system or program changes, QA will coordinate with appropriate staff to review and make necessary modifications.
2. QA will notify tester of approval to make or have modification/changes implemented.
3. Tester will retest failed test case/scenario.
4. If test case/scenario passes retest step, test case scenario will be marked as passed and completed.
5. If test case/scenario fails, QA will research reason for failure and work with necessary staff to resolve the issue/bug.
6. All issues/bugs will be documented into the QA Test Log database for tracking and reporting purposes.

A retesting process must occur before final approval:

- Any test case/scenarios that fail must be retested. All retests must take place in the same environment as the previous test with any modification/changes made to program and/or software. When test is completed, the retest date must be completed for tracking.
- All retest must be approved by QA before being logged as completed.

3.7. Final Review

Test Results are reviewed by all appropriate parties. A sample review checklist is provided below for reference:

System Interface	Resources	Area	Owners	Reviewers	Sign Off/Approval
MACESS	Claims Dept., MACESS Resource	Claims Dept.	Claims Dept.	MIS	Claims Dept., Plan
Translation/EDI	MIS Program., Claims Dept., CSS, MACESS resource	MIS Dept.	CSS	MIS Prog., Claims Dept., CSS, MACESS resource	Claims Dept., Plan
Claims - Regulation	CSS, MIS	CSS	CSS	CSS, Claims Dept.	CSS, Plan
Contracting	Contract Configuration Test Team, MIS	CCTT	CCTT	CSS, Claims Dept.	Plan
Letters	Claims Dept.	Claims Dept.	Claims Dept.	CSS, Provider Services	Communications Dept., Plan
Finance	MIS, Finance	Finance	Finance	Finance, MIS Dept., CSS	Plan